

بسم الله وبعد: تم الرفع بحمد الله من طرف

بن عيسى قرمزلي متخرج من جامعة المدية

تخصص: إعلام آلي

التخصص الثاني: حفظ التراث بنفس الجامعة

1983/08/28 بالمدية – الجزائر-

للتواصل وطلب المذكرات

هاتف : +213(0)771.08.79.69

بريدي إلكتروني: benaissa.inf@gmail.com

MSN: benaissa.inf@hotmail.com

فيس بوك: http://www.facebook.com/benaissa.inf

جامعــة الجــزائـــر (1)

كليـــــة الحقـــوق

الجرائم المعلوماتية في القانون الجزائري واليمني

أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق

فرع القانون الجنائي والعلوم الجنائية

إعداد الطالب	إشراف
فايز محمد راجح غلاب	الأستاذة الدكتورة/ نصرون وردية

أعضاء اللجنة

الأستاذ الدكتور /	أوهايبية عبد الله	رئيساً
الأستاذة الدكتورة/	نصرون وردية	مقرراً
الأستاذ الدكتور /	خوري عمر	عضواً
الأستاذة الدكتورة /	خالف عقيلة	عضواً
الأستاذ الدكتور /	مروك نصر الدين	عضواً

السنة الجامعية

2009/ 2010

{ اقْـرَأْ بِـاسْمِ رَبّـكَ الَّـذِي خَـلَقَ (1) خَـلَقَ
الإنـسَانَ مِـنْ عَـلَقٍ (2) اقْـرَأْ وَرَبّـكَ الأكْـرَمُ (3)
الَّـذِي عَـلّمَ بِـالْـقَـلَمِ (4) عَـلّمَ الإنـسَانَ مَـا لَـمْ
يَـعْـلَمْ (5) }

صدق الله الـعظيم

الآيات (من 1- 5) من سورة العلق

إهداء:

إلى والدي الفاضلين الذين مازالا مصدرا لإعانتي على مكابدة الحياة، ولا ينسياني من الدعاء.

إلى زوجتي وأولادي الذين صبروا على الفراق فترة غيابي أثناء الدراسة في بلدي الثاني الجزائر.

إلى إخواني الذين مازلت ألقى منهم المحبة والإعانة.

إلى كل من نصحني بمواصلة الدراسة

إلى كل مخلص وحريص على تحقيق الأمن والاستقرار

إلى كل من كان له أدنى فضل في إعانتي على إخراج هذا المجهود.

إليـهم جميعاً أهدي ثمرة هذا العمل

الشكر والتقدير

الشكر أولاً للخالق العلي المتعال الذي منه الإعانة والتوفيق، وعليه التوكل والحسبان، فهو نعم المولى ونعم النصير، ثم أشكر أستاذتي القديرة نصرون وردية، أستاذة التعليم العالي بكلية الحقوق – جامعة الجزائر- والتي تولت مهمة الإشراف على أطروحتي هذه، وأولتني الرعاية والاهتمام في إشرافها، حتى تم إخراجه بهذه الصورة، والشكر موصول لرئيس لجنة المناقشة الأستاذ الدكتور عبد الله أوهايبية وأعضاء اللجنة على قبولهم مناقشة هذه الأطروحة بالرغم من انشغالهم ووقتهم الثمين.

ولا يفوتني أن أشكر المديرية العامة للأمن الوطني بجمهورية الجزائر ممثلة بمديرية الشرطة القضائية، ونيابة مديرية الشرطة العلمية والتقنية، وعلى وجه الخصوص القسم المختص في استغلال الأدلة الرقمية على الفائدة العملية أثناء بقائي معهم في القسم، حيث بذل معي كل العاملين كل تعاون في مجال بعض التطبيقات العملية الفنية والتقنية المتعلقة بموضوع الدراسة، ولا أنسى من الشكر كل أساتذة كلية الحقوق وموظفيها، والعاملين في مكتبة الكلية، ومكتبة الماجستير، والدوريات، وقاعة الإنترنت، وكذلك العاملين في مكتبة الجامعة المركزية، وأشكر في الأخير دولة الجزائر على ما تقدمه من تسهيلات للدراسة فيها.

مــقدمـــــة

مما لاشك فيه أن استخدام الحاسب الآلي قد ارتبط بزيادة المعلومات التي فاقت طاقة الفكر الإنساني في متابعتها والاستفادة منها، نتيجة للتطورات الاقتصادية والاجتماعية، حيث بدت الطرق التقليدية لجمع وتنظيم المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفاعلية. وأصبح ضرورياً استخدام أساليب علمية وتقنية متطورة لمواجهة فيض هذه المعلومات، والتعامل معها، وتمثلت تلك الأساليب وتلك التقنية باستخدام الحاسب الآلي.

وفي بداية الأمر فقد تم استخدام الحاسبات الآلية من قبل المؤسسات العسكرية الروسية والأمريكية في كثير من الأعمال، منها تطوير وصناعة الأسلحة والصواريخ العابرة للقارات و كذلك السفن الحربية والفضائية وطائرات التجسس بدون طيار، وأعتبر آنذاك من الأسرار العسكرية.

ولم يدم استخدامأجهزة الحاسوب في المجال العسكري طويلاً ، فقد استخدمت في شتى المجالات المختلفة، ويعود ذلك إلى تزامن ثورة الحاسب الآلي والمعلوماتية وثورة الاتصالات، حيث نتج عن ارتباط المعلوماتية والاتصالات هذا التطور الملموس.

فلقد أزيلت الحدود الجغرافية أمام ذلك التطور، وأصبح بإمكان أي فرد لدية جهاز حاسوب موصول بشبكة المعلومات الدولية (الإنترنت) أن يتجول في هذا العالم الافتراضي، فيطلع على ما شاء من بيانات متاحة، ويعقد الصفقات، ويبيع، ويشتري، إلى غير ذلك من التعاملات، دون أن يتطلب الأمر الإجراءات التقليدية التي كانت معهودة من قبل، بحيث أصبحت معظم التعاملات تتم بواسطة الحاسوب، حتى أصبح العالم يعيش وكأنه في قرية واحدة، يتم تبادل المعلومات بين قاطنيه بسهولة ويسر، وقد وفر ذلك الكثير من الوقت والجهد وأعباء السفر.

ومع أن استخدام الحاسبات الآلية قد ساهمت في التطور الملموس بشتى مجالات الحياة، كما لعبت دورا هاما وحيويا لتطوير العمل الأمني في عدة أمور، منها تخزين المعلومات عن المجرمين وصفاتهم وصورهم وبصماتهم وأسلوبهم الإجرامي، إلى غير ذلك من البيانات التي لها علاقة بالمجرم والجريمة، ويمكن الرجوع إليها عند الحاجة بسهولة، إلا أنه قد رافق ذلك التطور وتلك التكنولوجيات ظهور أنواع جديدة من الجرائم

تتعلق بالمعلوماتية أطلق عليها بالجريمة المعلوماتية (Information crime)[1]، وقد تضاربت الآراء في تعريفها، اخترنا منها التعريف الذي أوردته منظمة التعاون الاقتصادي والتنمية عام 82، حيث عرفتها بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[2]، ويرجح هذا التعريف كونه يتميز بالوضوح أكثر من غيره، إضافة إلى تحديده للسلوك سواء كان فعلا ايجابيا أو سلبيا، وعدم اقتصاره على الأموال المادية فحسب، إضافة إلى كونه يستند إلى أكثر من معيار، وهو تعريف متبنى من قبل العديد من الفقهاء والدارسين بوصفه تعريفا واسعا يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، ولأنه يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، وكونه أخيرا يتيح إمكانية التعامل مع التطورات التقنية المستقبلية.

فهذه الجرائم أستخدم ولا يزال يستخدم في ارتكابها الحاسوب الآلي، وتستهدف فيها المعلومات، بالتجسس على البيانات المعالجة الكترونياً وسرقتها، وتدمير البرامج والبيانات، والاحتيال عليها، ونسخها، وتداولها بدون إذن منتجيها، ودس الفيروسات المعلوماتية التي تصيب الأنظمة بأنواع ودرجات متفاوتة من الأضرار، حتى أصبحت الجرائم المرتكبة بهذا الخصوص تشكل تهديداً بالغاً لسائر المنظمات الحكومية والخاصة التي تعتمد في تسيير أعمالها على النظم الإلكترونية.

ولم يقتصر الأمر على ما تحدثه تلك الجرائم من أضرار بالغة على أمن المجتمع واقتصاده، بل تعدت أضرارها الحدود الجغرافية فيما بين الدول، كونها لا تعترف بالحدود وقد ترتكب في أكثر من بلد.

([1]) ثار خلاف بين الفقهاء حول التسمية الأنسب للجرائم المرتكبة بواسطة التقنية الحديثة فمن الفقهاء من أطلق عليها بجرائم الكمبيوتر والانترنت، حيث أن الكمبيوتر والجرائم المرتبطة به ظهرت قبل الإنترنت، بينما سميت من قبل آخرين بجرائم الكمبيوتر لكون الجرائم التي ترتكب ولها علاقة بالشبكة ألعنكبوتيه إنما ترتكب عن طريق الحاسوب، وسميت بجرائم المعلوماتية وهي التسمية التي نراها مناسبة لكون هذه الجرائم تستهدف المعلومات، فأنماط السلوك الإجرامي تطال المعلومات المخزّنة، أو المعالجة في نظام الحاسوب أو المتبادلة عبر الشبكات، ولأن المعلومة تمثل أهمية قصوى لصاحبها فإن المفترض أن تشملها الحماية الجنائية، وخاصة بعد ظهور وتطور ثورة المعلومات في منتصف القرن العشرين و تبني فكرة بنوك المعلومات.

(2) راجع: احمد خليفه الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005، ص 97، هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، ط1، مكتبة الآلات الحديثة، أسيوط، 1992، ص 43.

كما أن طبيعة تلك الجرائم تؤثر على سير التحري والاستدلال وإجراءات التقاضي، لظهور عدد من المشكلات الإجرائية، منها سهولة وسرعة إخفاء أثارها، وتعديها نطاق الاختصاص المحلي والدولي، وما يترتب على ذلك من تنازع في الاختصاصات والقوانين الواجبة التطبيق عليها، في ظل عدم وجود تعاون دولي، ومدى تناسب الإجراءات التقليدية المتعلقة بالتحري والتحقيق والمحاكمة في مكافحتها، وكذلك حجية الأدلة المتحصلة عنها في الإثبات.

وأمام هذا الشكل الجديد لتلك الجرائم، والصعوبات التي تواجه متابعتها وضبط مرتكبيها، فقد أصبحت بعض نصوص القوانين التقليدية في شقيها الموضوعي والإجرائي لا تفي بمواجهتها، ولا تتناسب مع التكييف القانوني لها، لكونها كانت تتعامل مع الثروة الملموسة والمستندات ذات الطبيعة المادية، مما يتعذر تطبيقها لحماية القيم المتولدة عن المعلوماتية، ولكون نصوص قانوني العقوبات والإجراءات موروثة بعضها من القرن التاسع عشر، حيث لم يكن يوجد آنذاك فنيين، وإنما حرفيون وأصحاب مهن، وتطبيق تلك القوانين على الأشكال الجديدة للجرائم المعلوماتية التي تعتمد على تقنية الحاسوب يصطدم بصعوبات ناجمة عن الطبيعة الخاصة للخصائص التقنية المستخدمة في ارتكابها، و التي يلم بها مرتكبو تلك الجرائم وتمكنهم من إخفاء آثارها أو محوها أو التلاعب بها، مما يستدعي إعادة النظر بإصدار تشريعات تتناسب مع أركان الجريمة المعلوماتية، والطبيعة الخاصة المتميزة والمتفردة بها، وتمكن سلطات تحقيق العدالة من التعامل معها، بحيث توسع من الإجراءات التي تعتمد على الجوانب الفنية والتقنية، والتي تتطلب أن تكون الأجهزة المنفذة لها مدربة تدريباً عالياً ونوعياً يمكنها من القيام بها.

وإزاء ذلك فقد عقدت المؤتمرات الإقليمية والدولية، لمناقشة خطورة هذه الجرائم، ووضعت التوصيات التي تعني بوضع التشريعات التي تتناسب مع حداثة تلك الجرائم، وأهمية التعاون الدولي في مكافحتها، كما وقعت الاتفاقيات الدولية بهذا الخصوص.

وقد تباينت الآراء وتضاربت، حول القواعد التي يجب على المشرعين إتباعها لوضع تشريعات مناسبة ومعاصرة، لكن التقدم السريع والمستمر لهذه الشبكة جعلها

تسبق حركة المشرعين، كما جعلها تتخطى القواعد القانونية الموضوعة لتنظيمها، مما دفع المشرعين إلى وضع قواعد عامة يتم اللجوء إليها عند ظهور أي خرق أو تعد.

وأمام هذه الحركة التشريعية فما زالت أغلب الدول العربية تكيف التطورات الناشئة عن التقدم التكنولوجي مع بعض تشريعاتها وقوانينها الداخلية التقليدية. وعمدت على تنظيم عقاب ومكافحة هذا النوع من الإجرام بواسطة النصوص التقليدية [1].

وبخلاف ذلك فقد عملت دول أخرى على إضفاء نصوص قانونية ألحقتها بقانون العقوبات مثل فرنسا، و سلطنة عمان، والجزائر، وقطر، وما زال القصور يفتقر للجانب الإجرائي في بعض هذه الدول [2].

كما عمدت دول أخرى إلى إيجاد تشريعات خاصة تنظم هذا النوع من الإجرام المستحدث ومنها بريطانيا، والمملكة العربية السعودية، والإمارات العربية المتحدة [3].

وبناء على ما سبق فإن إشكالية البحث تتمثل في التساؤل الآتي:

هل النصوص القانونية التقليدية موضوعية كانت أو إجرائية تفي بمواجهة الجرائم المعلوماتية التقليدية منها والمستحدثة؟ أم أن مقتضيات الضرورة وطبيعة تلك الجرائم تحتاج إلى مواجهتها من خلال نصوص أو قوانين مستحدثة؟

وهذا التساؤل بدوره يمكن أن يتفرع إلى العديد من الاستفسارات منها:

- هل الجرائم المعلوماتية التقليدية والتي منها الجرائم الماسة بالأمن القومي للدولة، وجرائم الأموال، وغيرها تتفق في أركانها مع الجرائم التقليدية الصرفة؟
- هل المعلوماتية مالاً منقولاً مملوكاً للغير؟ وهل تتفق وطبيعة المال في الجرائم التقليدية حتى يمكن القول بتحقق جرائم الأموال في نطاق المعلوماتية؟

([1]) ومن تلك الدول التي مازالت تفتقر إلى النصوص المستحدثة في مواجهة الجرائم المعلوماتية موضوعيا وإجرائيا، الجمهورية اليمنية، وجمهورية مصر العربية، والأردن، والبحرين، والكويت، والسودان، وسوريا، وجيبوتي، والصومال، وغيرها من الدول.

([2]) ومن تلك القوانين التي تضمنت نصوص قانونية لمواجهة جرائم المعلوماتية، قانون العقوبات الفرنسي لعام 1988 والذي تعديله في 1 / 3 / 1994، ومن بعد2004، وكذلك المرسوم السلطاني رقم(72/ 2001) والذي تضمن تعديل بعض أحكام قانون الجزاء العماني وإدخال جرائم الحاسوب، وقانون العقوبات الجزائري من خلال تعيل 2004، بموجب القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004، وكذلك قانون العقوبات القطري رقم(11)لسنة 2004، حيث تضمن الفصل الخامس جرائم الحاسب الآلي.

([3]) ومن التشريعات المستقلة التي نصت على جرائم المعلوماتية، قانون إساءة استخدام الحاسب في المملكة المتحدة لعام 1991، وكذلك القانون الإماراتي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، ونظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم(م/17) المؤرخ في 1428/3/8هـ بناء على قرار مجلس الوزراء رقم (79)المؤرخ في 1428/3/7هـ، الموافق 2007/3/6.

- هل النصوص القانونية التقليدية يمكن تطبيقها على الجرائم المعلوماتية المستحدثة؟ أم أن حداثة تلك الجرائم وارتباطها بأفعال ذات طابع تقني تحتاج إلى نصوص قانونية تتناسب معها؟

- هل القواعد التي تحكم الدخول في مسكن خاص يمكن تطبيقها على الدخول إلى نظام المعالجة الآلية للمعطيات ؟

- هل يمكن قياس الإتلاف التي تتعرض له المعطيات بالمحو، أو التعديل، أو التلاعب، وكذلك تخريب النظام، أو إعاقته، على إتلاف الأشياء المادية؟

- ما مدى تطبيق القوانين الإجرائية التقليدية على إجراءات التحري والتحقيق والمحاكمة في جرائم المعلوماتية في ظل عدم تقيد هذه الجرائم بحدود جغرافية، وقصور في التعاون الدولي، وسرعة إخفاء الأدلة وطبيعتها غير المادية؟ أم أنها تحتاج إلى إجراءات إضافية تتناسب مع الجوانب التقنية لتلك الجرائم تتضمنها نصوص قانونية جديدة وتعديل بعض النصوص التقليدية؟

- هل بإمكان جهات تحقيق العدالة القيام بالتفتيش والضبط لأجهزة الحاسوب عن بعد؟ وما مدى شرعية الإجراءات التي تتخذ في الملاحقة والضبط والتفتيش خارج نطاق الاختصاص المكاني المحلي والدولي ؟

- هل الدليل الإلكتروني له نفس حجية الإثبات كالدليل التقليدي، أم أن المسألة بحاجة إلى إعادة نظر في هذه التشريعات؟

- هل بإمكان أي دولة القيام بأي إجراء مما ذكر عن بعد دون وجود تعاون دولي؟

وحسب ما تم ذكره في الإشكالية المشار إليها، وحتى يتم الإجابة على تلك التساؤلات وغيرها مما يتعلق بحداثة تلك الجرائم وما رافقتها من مشكلات فقد وضعت عدد من الفرضيات تثبتها أو تنفيها الدراسة منها:

- النصوص التقليدية في قانون العقوبات اليمني والجزائري تفي لمواجهة الجرائم التقليدية المرتكبة بواسطة المعلوماتية، ومنها الجرائم الماسة بالأمن القومي للدولة ويفضل إجراء بعض التعديلات عليها.
- المال المعلوماتي ذو طبيعة مادية قابل للنقل والتملك مثل المال المادي.

- يمكن تطبيق النصوص القانونية التقليدية الخاصة بجريمتي السرقة والنصب على سرقة المعلومات المخزنة في نظام المعالجة الآلية للمعطيات، وكذا جريمة الاحتيال الالكتروني.
- جريمة الدخول إلى نظام المعالجة الآلية للمعطيات هي بمثابة جريمة الدخول إلى مسكن خاص، ولذا يمكن أن تطبق عليها العقوبة نفسها.
- تختلف جريمة الإتلاف المادية عن جريمة الإتلاف في مجال المعلوماتية.
- يمكن تطبيق القواعد العامة الخاصة بالتحري والتحقيق والمحاكمة على مكافحة جرائم المعلوماتية مع مراعاة بعض الخصوصيات ذات الطابع التقني والتي تحتاج إما إلى نصوص مستحدثة تنظمها، أو تعدل النصوص القائمة.
- يمكن الاعتماد على الدليل الالكتروني، واعتباره حجة في الإثبات، مثله مثل الدليل المادي.
- لابد لأجهزة تحقيق العدالة من تدريب تخصصي في الجوانب الفنية المتعلقة بمهامها الإجرائية حتى تقوم بتلك المهام بفاعلية وتحقق نتائج ايجابية.
- لا يمكن القيام بأي إجراء تقني يتعلق بعمل ذي طابع قضائي عن بعد وخارج إقليم الدولة دون تعاون وتنسيق دولي.

وتبدو أهمية هذه الدراسة وسبب اختيارنا للموضوع، للتعريف بجرائم ارتبطت بتطور المجتمعات وتقدمها، حيث أن زيادة الاعتماد على الحاسبات الآلية وارتباطها بتكنولوجيات الاتصالات والمعلوماتية، جعلت أغلب الخدمات تسيرها أنظمة إلكترونية، وكان ذلك سبباً في زيادة ارتكاب هذه الجرائم، لذلك كان من الضروري أن يستتبع ذلك فهماً لمواجهتها من الناحية القانونية، خاصة بعد صدور تشريع خاص بها في الجزائر الذي مازال يفتقر إلى شرح وإيضاح، كما زاد من أهمية هذه الدراسة عدم وجود قانون يمني يعني بمواجهتها موضوعياً وإجرائياً ، وتهدف الدراسة إلى تنبيه المُشرِّع اليمني بضرورة مسايرة التشريعات الحديثة في مجال مكافحة الجرائم المعلوماتية ومنها التشريع الجزائري وبعض التشريعات العربية الأخرى ناهيك عن أغلب القوانين الأجنبية.

ولم تكن هذه الدراسة هي الأولى في هذا المجال، فلقد تناولت هذا الموضوع عدد من الدراسات، إلا أنه يمكن القول بأن تلك الدراسات تركزت بصفة أساسية على الدول

المتقدمة في المجال الرقمي،نظراً لظهور تلك الجرائم بشكل ملفت للنظر متزامنة مع ذلك التطور، مما جعل فقهاء القانون في تلك الدول يتناولون هذا الموضوع بالشرح والتوضيح، بخلاف أساتذة القانون في البلدان العربية، حيث تناولت معظم تلك الدراسات لهذا الموضوع بشكل عام، محاولة إيجاد تقسيمات لها، والتعرف على أهمها، معتمدة على القوانين والمراجع الأجنبية، وقد حاول بعض منهم أن يكيف النصوص التقليدية لكي تنطبق على هذه الجرائم، بينما حاول البعض الآخر أن يخرج بنتيجة تتمثل بعدم ملائمة النصوص التقليدية للانطباق عليها، ومن تلك الدراسات:

- دراسة بعنوان: الجرائم الناشئة عن استخدام الإنترنت، وهي رسالة دكتوراه أعدها عمر محمد أبو بكر يونس قدمت لجامعة القاهرة، 2004، تناولت الجوانب الموضوعية والإجرائية للجرائم الناشئة عن استخدام الإنترنت بشكل عام .
- رسالة دكتوراه بعنوان: جرائم الحاسب الآلي الاقتصادية قدمت من نائلة عادل محمد فريد قوره إلى جامعة القاهرة في 2004، تناولت الأحكام العامة لجرائم الحاسب الآلي، ومدى صلاحية النصوص التقليدية للانطباق عليها، حيث اعتمدت على دراسة القانون المقارن نظراً لعدم وجود قانون مصري في مجال جرائم المعلوماتية.
- دراسة مقدمة من أحمد خليفة الملط تحت عنوان: الجرائم المعلوماتية، 2005، وهذه الدراسة كسابقاتها تناولت الجرائم المعلوماتية بشكل عام وكان المؤلف في أغلب الأحوال يتبنى الرأي القائل بإمكانية تطبيق النصوص التقليدية على تلك الجرائم.
- دراسة بعنوان: الجرائم الناشئة عن استخدام الحاسب الآلي، ومؤلفها أحمد حسام طه تمام ، 2000، تناولت عدداً من الجرائم التقليدية وأخرى مستحدثة، وقد دخلت في تفاصيل تغلب الجوانب الفنية على القانونية.
- دراسة بعنوان: الانترنت والقانون الجنائي، جميل عبد الباقي الصغير –الأحكام الموضوعية لجرائم الانترنت، القاهرة،2002، وهي كذلك تناولت الموضوع بشكل عام.

- دراسة بعنوان: التفتيش الجنائي على نظم الحاسوب والإنترنت لـ علي حسن محمد الطوالبة، وهي رسالة دكتوراه مقدمة لجامعة عمان العربية للدراسات العليا، تناولت جزئية في الجانب الإجرائي لجرائم المعلوماتية دون التطرق للجوانب الأخرى.

فهذه الدراسات وغيرها التي توافرت لنا، قد تناولت الجرائم المعلوماتية بشكل عام معتمدة على القوانين والمراجع الأجنبية، بحيث لم تتطرق أي منها لبيان الأحكام الخاصة لكل جريمة في ضوء قانون عربي مستحدث لمكافحة جرائم المعلوماتية، مع أن بعض القوانين كانت قد صدرت في هذا المجال، ولتأخر المشرع العربي في بعض الدول العربية الأخرى في إصدار مثل تلك القوانين.

إضافة إلى أن الدراسات التي تناولت الجانب الموضوعي تزيد بكثير عن التي تناولت الجانب الإجرائي.

وجديد هذه الدراسة أنها لا تتناول الموضوع بشكل عام فحسب؛ بل تتناوله بالشرح والمقارنة لبيان الأحكام الخاصة لأهم تلك الجرائم تقليدية كانت أو مستحدثة، مع عدم إغفال ما يخص الجانب الإجرائي من خلال قانونين أحدهما مستحدث تناولها بنصوص جديدة وما زال خالياً من الشرح وهو القانون الجزائري، والآخر القانون اليمني الذي مازال بصيغته التقليدية التي قد لا تفي بتحقيق الحماية الجنائية لتلك الجرائم .

وسيتم الاعتماد في هذه الدراسة على : المنهج التحليلي الوصفي، وذلك بالاعتماد على مراجع باللغة العربية وبعض المراجع باللغة الأجنبية، كما سيتم الاستعانة بالإنترنت للترجمة، ومتابعة المواقع الخاصة بجرائم الحاسوب لمعرفة كل جديد يتعلق بالموضوع وتضمينه هذه الدراسة،نظراً لحداثة هذه الجرائم وتطورها، كذلك سيتم التطرق إلى المنهج المقارن من خلال المقارنة بين القانون الجزائري واليمني بشكل خاص، وبعض القوانين الأخرى على سبيل الاسترشاد، ولا يفوتنا أأن نسلك المنهج التاريخي وإن كان ذلك بصورة مقتضبة لبيان التطور التاريخي للحاسوب والإنترنت.

وهذه المنهجية اتبعناها لتفادي الصعوبات التي قد تعترض هذه الدراسة والتي منها:

قله المراجع المتعلقة بالموضوع باللغة العربية، بالإضافة إلى أن أغلب هذه المراجع مصادرها أجنبية، وكذلك الاعتماد على بعض المراجع باللغة الأجنبية وخاصة

الفرنسية وما يترتب على ذلك من جهد في ترجمتها، والأخطاء التي قد ترافق ذلك مستعيناً بمواقع الترجمة وبعض الزملاء الجزائريين، كما أن من الصعوبات التي تواجه هذه الدراسة تلك المتعلقة بالجوانب الفنية ذات العلاقة بالمدلول القانوني في هذه الجرائم، لكون الباحث وغيره من خريجي الجامعات العربية في مجال الحقوق لم يتلقوا مثل هذه العلوم العصرية التي أظهرتها التكنولوجيا الرقمية وارتبطت بالجانب القانوني، كذلك من ضمن الصعوبات التي جعلت الباحث يغير بل ويعدل من صياغة بعض العناوين والفقرات، بحيث أن بعض الأمور التي كانت مبنية على النفي تصبح بعد ظهور تشريعات جديدة مبنية على الإثبات، ويزيد من تلك الصعوبات أن يظهر تشريع جزائري جديد والباحث على وشك تسليم أطروحته للمجلس العلمي مما يجعله يعيد النظر فيها ويعمل على تضمينها ذلك القانون [1]، بل إن القانون الفرنسي المتعلق بهذه المسألة لعام 2004 لم تشر إليه كافة المراجع التي تحصلت عليها، وكان للانترنت الفضل في تعريفي به.

وبناء على ما تم بيانه فقد ارتأيت تقسيم خطة هذه الدراسة إلى بابين:

- **الباب الأول**: يتناول أهم الجرائم المعلوماتية من خلال فصلين اثنين، يتناول **الفصل الأول:** أهم الجرائم المعلوماتية التقليدية المرتكبة بواسطة المعلوماتية، والتي منها الجرائم المتعلقة بالأمن القومي للدولة، وجرائم الأموال في نطاق المعلوماتية، بينما يتناول **الفصل الثاني**: الجرائم المعلوماتية المستحدثة.

- **الباب الثاني**: ويتم من خلاله بيان المشكلات الإجرائية لجرائم المعلوماتية، وذلك في فصلين، يتناول **الفصل الأول**: المشكلات الإجرائية المتعلقة بالتحري والتحقيق في جرائم المعلوماتية، ويتناول **الفصل الثاني**: المشكلات المتعلقة بالاختصاص القضائي وحجية الدليل الإلكتروني في الإثبات ودور التعاون الدولي في معالجة تلك المشكلات.

([1]) بعد صدور القانون الجزائري رقم (04- 15) المؤرخ في 10 نوفمبر 2004 بخصوص المساس بأنظمة المعالجة الآلية للمعطيات المُعَدِل والمُتَمِم للأمر رقم (66- 156) المؤرخ في 8يونيو 1966 يتضمن قانون العقوبات، حيث وأن النصوص التي تضمنها هذا القانون قد وضعت لمواجهة الجرائم المعلوماتية المنصوص عليها من ناحية موضوعية، فقد عمل المشرع الجزائري على تعديل وتتميم الأمر رقم (66- 156) المؤرخ في 8يونيو 1966 المتضمن قانون الإجراءات الجزائية بالقانون رقم (06- 22) المؤرخ في 20 ديسمبر 2006، وكان من ضمن ما تضمنه نصوص تتعلق بتوسيع بعض الصلاحيات والإجراءات في مجال مكافحة جرائم المعلوماتية، وفي 5 غشت(أغسطس) 2009 اصدر المشرع الجزائري القانون رقم (09- 04) يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الباب الأول

أهم الجرائم المعلوماتية في القانون الجزائري واليمني

الباب الأول

أهم الجرائم المعلوماتية في القانون الجزائري واليمني

نتج عن التطور التكنولوجي في مجال الحاسوب(1). والأنظمة المعلوماتية، وأنظمة الاتصالات بما في ذلك شبكة الإنترنت مزايا متعددة في شتى مجالات الحياة المختلفة، بحيث لا يمكن إنكارها(2).

إلا أن ذلك التطور وتلك التقنية لم تسلم من الهجوم عليها، فظهرت أنوع جديدة من الجرائم سميت بالجرائم المعلوماتية، منها جرائم كانت معروفة تحت مسميات تقليدية، حيث كانت تقترف قبل ظهور الحاسوب، والأنظمة المعلوماتية وأنظمة الاتصالات وتطورهما، وأصبحت بعد ظهور وتطور تلك الأنظمة ترتكب بوسائل وتكنولوجيا لم تكن معروفة من قبل، فازدهرت بذلك عملية التجسس على المعلومات المعالجة آليا، وسرقتها، حتى أصبحت تمثل تهديدا بالغ الخطورة لسائر المؤسسات والمنظمات

([1]) قديما عرف الحاسب لغة بان مصدره الفعل حسب أو نحوه، وعلم ألحاسب وهو علم العد والتدبير والتدقيق، وتعني كلمة الحاسب حاسوب، كما أطلق عليها عقل اكتروني، وأخيرا أطلق عليها حاسب، وبالانجليزية (computer)وبالفرنسية (Ordinateur)، ويعد الكمبيوتر ايناك (ENIAC) هو أول كمبيوتر الكتروني اخترعه بريسر أكرت Prespe recke وجون موكلي(john mauchly)من جامعة بنسلفانيا وكان جهاز متعدد الأغراض قادر على جمع 5000 عملية جمع في الثانية الواحدة وكان يبلغ وزنه 30 طن ويشغل مساحة 7×15 متر مربع وكان يعمل بالدوائر الكهربائية، وتصدر عنه طاقه حرارية فكان المكان الذي يتواجد به محاط بالمبردات، وقد استخدم بداية في المجال العسكري، وقد تم تطوير الحاسوب سواء من حيث حجمه الصغير أو من حيث الخدمات التي يقوم بها، حتى أصبح بالحجم الذي نراه اليوم، بحيث يكون بإمكان كل فرد أن يأخذه معه، ومع ذلك فإنه لا يقارن بخدماته السريعة والمتطورة، والمتعددة مقارنة بالحواسيب في بداية اختراعها. راجع في التعريف: المعجم الوجيز – مجمع اللغة العربية – وزارة التربية والتعليم بجمهورية مصر العربية ط 1995 ص17، وفي المصطلحات الغوية للحاسوب راجع: احمد خليفه الملط، الجريمة المعلوماتية، دار الفكر الجامعي الإسكندرية، 2000، ص25، وفي تطوير الحاسوب راجع: أنطوان بطرس، موسوعة الكمبيوتر، ط2 ، مكتبة لبنان، 1994، ص20، وفي الاستخدام راجع: محمد على العريان ، انعكاس ثورة المعلومات على قانون العقوبات، دار الجامعة للنشر،الإسكندرية 2004، ص72.

(2) ظهرت مزايا كثيرة لاستخدام الأنظمة المعلوماتية في شتى مجالات الحياة على مستوى الفرد والمؤسسة والدولة، فلم يعد بالإمكان الاستغناء عن تلك التكنولوجيا، وعلى سبيل المثال فإن التجارة الإلكترونية تتيح عبر الإنترنت عمليات دعم المبيعات وخدمة العملاء، ويمكن تشبيهها بسوق إلكترونية يتواصل فيها البائعون – موردون، أو شركات، أو محلات ، أو الوسطاء، أو السماسرة- أو المشترون، وتقدم فيها الخدمات في صيغة افتراضية أو رقمية، كما يدفع ثمنها بالنقود الإلكترونية. كما أن التلفون التقليدي الذي كان يقتصر عمله على تبادل الصوت البشري، قد أصبح بإمكانه تبادل كميات هائلة من البيانات التي يمكن أن تحوي أصوات ونصوص وصور وأفلام، وهذا التبادل لم يعد بين البشر فحسب، بل بين البشر وأجهزة الحاسوب، وأجهزة الحاسوب فيما بينها، كذلك يكفي أن يتم إدخال البيانات إلى شبكة معينة حتى تصبح متوافرة لأي شخص يريد الدخول إليها، كما أن الاستخدام العام للبريد الالكتروني، ووصول المستخدمين لمواقع الويب أمثلة بسيطة لهذا التطور. راجع: هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23نوفمبر2001، ط1، دار النهضة العربية، القاهرة، 2003، ص31. وراجع: محمد الصيرفي، الإدارة الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص168.

الحكومية والخاصة وتفضي إلى خسائر اقتصادية كبيرة[1]، بل إنها أضحت تمثل تهديدا على حياة وخصوصيات الأفراد، وحقوقهم الأدبية الفكرية.

وبمعنى آخر فإن كافة الجرائم التقليدية سواء أكانت تمس الأمن القومي للدولة أم تمس حياة وخصوصيات الأفراد، مثل جرائم الاعتداء على الأشخاص، أو الاعتداء على الأموال، أو الاعتداء على الأعراض يمكن ارتكابها بواسطة نظم المعلوماتية.

ونتيجة لذلك فقد ظهرت بعض الإشكاليات التي تتعلق بتكييف تلك الجرائم، حيث انقسم الفقه المعاصر في بيان حكمها إلى اتجاهين[2]:

اتجاه يرى: عدم ضرورة التفرقة بين الجرائم التي ترتبط بالحاسب الآلي، وتلك التي لا ترتبط به، فالحاسب الآلي ما هو إلا وسيلة لارتكاب جريمة معاقب عليها بالفعل بواسطة النصوص القائمة.

بينما يرى الاتجاه الآخر: بضرورة التدخل التشريعي لمواجهة الجرائم المعلوماتية، نظراً لما تتميز به عن غيرها من الجرائم.

وإضافة إلى الجرائم التقليدية التي يمكن ارتكابها بواسطة المعلوماتية- والتي سيتم تناولها في الفصل الأول من هذا الباب- فقد ظهر نوع جديد من الجرائم يمكن أن يطلق عليه الجرائم المعلوماتية المستحدثة[3].

([1]) شهد العالم خلال عام 2004 ما يقرب من 180 ألف هجوم إلكتروني تسببت في خسائر اقتصادية تتراوح مابين80 إلى 100 مليار $، وتعد البلدان الأكثر تضررا هي الدول المتقدمة في مجال التقنية. راجع: مجلة تكنولوجيا الاتصالات والمعلومات، صادرة عن وزارة الاتصالات وتقنية المعلومات اليمنية، ع42، ديسمبر 2003، ص3.

2) راجع نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، رسالة كتوراة، جامعة القاهرة، ط1، منشورات الحلبي الحقوقية، لبنان، 2005، ص305.

([3]) ظهرت أول معالجه لما يسمى بجرائم الكمبيوتر في الستينات والسبعينات لأكنها اقتصرت على مواد صحفيه ومقالات تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر،ورافق ذلك نقاشات حول ماذا كانت هذه الجرائم مجرد شيْ عابر، أم ظاهره جرميه مستحدثه، بل ثار الجدال حول ماذا كانت جرائم بالمعنى القانوني، أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، وبقي التعامل معها اقرب إلى النطاق الأخلاقي من القانوني، وفي الثمانينات ظهر مفهوم جديد لجرائم الكمبيوتر ارتبط بعملية اقتحام نظم الكمبيوتر عن بعد، وأنشطة نشر زراعة الفيروسات، وشاع اصطلاح الهاكرز مقتحمي النظم، إلا أن دوافعهم ظلت محصورة في رغبة المحترفين تجاوز إجراءات امن المعلومات، وفي مرحلة ثالثة في التسعينات حدث تنامي هائل في جعلها جرائم التقنية، وتغير نظامها ومفهومها بفعل ما أحدثته شبكة الانترنت وظهرت أنشطه جديدة استهدفت فيها المواقع الإلكترونية، وسهل ذلك التطور سرعة نشر الفيروسات عبر الشبكة راجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 38.

وقد ظهرت هذه الجرائم وتطورت بظهور وتطور تكنولوجيات الإعلام والاتصال، وقد فاقت مخاطر هذه الجرائم المخاطر الناتجة عن الجرائم المرتكبة بالوسائل التقليدية، بسبب الاعتماد الكبير في مجال المعاملات بشتى أنواعها على الوسائل الالكترونية في تسييرها.

وبالتالي فإن اعتداء ما على نظم معلوماتية لتسيير جوانب خدماتية في المجتمع، مثل الكهرباء أو الصرف الصحي وغيرها، قد يتسبب في كارثة بيئة.

ويتم ارتكاب تلك الجرائم من خلال الاعتداء على نظم المعلوماتية، أو على المعلومات المدرجة بتلك النظم، ومن تلك الجرائم، جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات، وجريمة الاعتداء على البيانات المدرجة بنظم المعلوماتية، وجريمة التعامل غير المشروع مع المعطيات الناتجة عن جرائم المعلوماتية، أو التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية، وغيرها من الجرائم التي سنتناولها في الفصل الثاني من هذا الباب.

الفصل الأول

الجرائم التقليدية المرتِكبة بواسطة المعلوماتية

تكاد كل الجرائم التقليدية ترتكب بواسطة نظم المعلوماتية، وهذه الجرائم منصوص عليها في القوانين العقابية التقليدية، ويطلق عليها بذات الأسماء التي تطلق على الجرائم التقليدية، فقد تكون من الجرائم الماسة بأمن الدولة، أو من جرائم الاعتداء على الحياة الخاصة، أو الملكية الفكرية، وقد تكون من الجرائم المتعلقة بالجوانب الإباحية، فقد تكون الجريمة المرتكبة جريمة قتل[1]، أو جريمة قذف، أو من جرائم الأموال، مع عدم التفرقة بين جرائم الأموال أو الأشخاص في مجال المعلوماتية[2].

ومع أن التكنولوجيا الرقمية، ودخول الحاسب الآلي قد ساعدت في عمليات التجارة الإلكترونية وتحويل الأموال، فقد استخدمت في اقتراف تلك الجرائم بما فيها جرائم ذوي الياقات البيضاء [3].

وإذا كانت الجرائم المعلوماتية المستحدثة تتطلب المواجهة القانونية وفق نصوص مستحدثة وفقا لما سوف يتم تناوله أثناء إيضاح تلك الجرائم، فهل الجرائم التقليدية المرتكبة بواسطة المعلوماتية تحتاج كذلك إلى قوانين تتناسب مع تلك الجرائم والوسائل المرتكبة بواسطتها؟ أم أن النصوص التقليدية تفي بمواجهتها؟ يأتي هذا التساؤل في ظل الإشكالية التي تكمن في التكييف القانوني للجريمة التقليدية المرتكبة بواسطة المعلوماتية في ظل اختلاف طبيعة الأموال في الجريمة التقليدية المعلوماتية عن الأموال في الجريمة التقليدية الصرفة، فالأموال في الثانية ذات طبيعة مادية بينما في الأولى ذات طبيعة معنوية، كما أن الوسائل والأفعال التي تقترف فيها تلك الجرائم تعتمد على التقنيات الحديثة وهي بذلك تختلف عن الوسائل والأفعال التقليدية.

---

(1) ومن قضايا القتل التي حدثت في مجال المعلوماتية قيام شخص بقتل زوجته عمدا عن طريق دخوله على الشبكة الداخلية للمستشفى ومن ثم قيامه بتغير الوصفات الطبية الخاصة بزوجته المريضة على نحو قاتل ،وحين أعطيت لها الأدوية من قبل الممرضة ماتت المريضة، فمثل هذه الجريمة تعد جريمة قتل عمد تمت بواسطة تعديل البيانات في نظام المعالجة الآلية للمعطيات في المستشفى. راجع عبد الفتاح بيومي حجازي، الأحداث والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2002، ص244، محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسوب الآلي والانترنت، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص48.

(2) نصرون وردية، جريمة الغش في الإعلام الآلي، المجلة القضائية، المحكمة العليا، الجزائر، ع1،2002، ص110.

(3) عادل الطبطبائي، ((جرائم ذوي الياقات البيضاء))، مجلة الحقوق الكويتية، فصلية علمية محكمة، ع3، س23، سبتمبر 1999، ص284.

و سيتم الاقتصار في هذا الفصل على جرائم الاعتداء على الأمن القومي للدولة نظرا لما تمثل من خطورة في ظل التطور الرقمي الذي سهل للدول المتقدمة التجسس على الدول الأخرى عن طريق شبكات إلكترونية وضعت لهذا الأساس[1]، وكذلك جرائم الإرهاب، وغسيل الأموال، والمخدرات .

كما سيتم تناول جرائم الاعتداء على الأموال في مجال المعلوماتية، حيث سيتم تناول جريمتي السرقة والنصب.

---

(1)كشف أخيرا النقاب عن شبكة دولية ضخمة للتجسس الالكتروني تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا،وبريطانيا، واستراليا ونيوزيلندا ويطلق عليها اسم (ECHELON) لرصد المكالمات الهاتفية والرسائل بكافة أنواعها سواء ما كان منها برقيا، أم تلكسيا، أم فاكسيا أم إلكترونيا،عن طريق اعتراض كميات هائلة جدا من الاتصالات والرسائل الإلكترونية عشوائيا باستخدام خاصية الكلمة بواسطة الحاسوبات المتعددة، حيث تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية، منها محطة رصد الأقمار الصناعية الواقعة في منطقه بجنوب نيوزيلندا، ومحطة موجودة باستراليا، والمحطة الموجودة في مقاطعة كورن وول ببريطانيا، والمحطة الواقعة في الولايات المتحدة الأمريكية (250) كيلومترا جنوب واشنطن ، وأيضا المحطة الموجودة بولاية واشنطن على بعد(200) كيلومتر جنوب غرب مدينة سياتل. ولا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية، بل يشمل رصد الاتصالات التي تجرى عبر أنظمة الاتصالات الأرضية وكذا الشبكات الإلكترونية، حيث أصبح الأفراد والمنظمات والحكومات اللذين لا يستخدمون أنظمة الشفرة التأمينية، أو أنظمة كودية لحماية شبكاتهم وأجهزتهم أهدافا سهلة لشبكة التجسس، ولا يعنى هذا أن الأهداف التي تستخدم أنظمة الشفرة في مأمن تام من التجسس عليها، إذ يكون بإمكان مجرمي المعلوماتية فك التشفير والاكواد الموضوعة، كما أن التجسس الالكتروني لا يقتصر على المعلومات العسكرية أو السياسية بل يتعداه إلى المعلومات التجارية والاقتصادية والثقافية.وبهذا الصدد تفيد تقارير عديدة، عن وجود محاولات من وكالات الاستخبارات العالمية، للتجسس على مستخدمي الإنترنت في العالم، مثل الكشف عن ارتباط مفتاح أنظمة ويندوز بوكالة الأمن القومي الأمريكية (NSA) ، ليسمح لها بجمع المعلومات عن جميع مستخدمي نظام ويندوز، عبر الإنترنت. راجع: منير محمد الجنبيهي ومحمود محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي، الإسكندرية،2004، ص78. وراجع: محمد عبدا لله المنشاوي، المخاطر الأمنية للإنترنت، بحث منشور على موقع المنشاوي للدراسات والبحوث، ت.د 2009/9/10، على الرابط:

http://www.minshawi.com/old/internet-crime.htm

وراجع أيضا: عايض المري، أمن المعلومات - ماهيتها وعناصرها وإستراتيجيتها، بحث منشور على موقع الدكتور المري، ت.د 2008/6/11على الرابط:

http://www.dralmarri.com/show.asp?field=res_a&id=205

و بخصوص ارتباط نظام ويندوز بوكالة الاستخبارات الأمريكية، راجع اللواء صلاح الدين سليم الخبير بأكاديمية ناصر العسكرية، مصر، صحيفة الإخبارية الالكترونية، 05-05-2006، تم التأكد من أن الموضوع مازال منشور في موقع الصحيفة في 30/ 2009/9:على الرابط :

http://www.sharesgate.com/vb/t5856.html

المبحث الأول

الجرائم الماسة بالأمن القومي للدولة

نظرا لاعتماد المؤسسات الحكومية والخاصة على نظم الحاسوب نتيجة لتعميم المعلوماتية، وأن هذه المعلومات ذات القيمة قد أضحت معالجة ومخزنة بواسطة نظم المعلوماتية، فإن بعدا جديدا من تهديد المجتمع قد أصبح واردا ، فما يقع من أنشطة إجرامية تستهدف نظم الحاسوب يمكن أن يكون لها تأثير خطير على سير المجتمع وأداء المؤسسات مع فارق كبير عما كانت عليه النظم اليدوية، بالإضافة إلى أن تركيز المعلومات المتعلقة بالأفراد والمؤسسات وسائر الأنشطة الحيوية المتعلقة بالمجتمعات والأنظمة في منظومات الحاسوب، من شأن ذلك أن يوسع من حجم المشكلة ويعتبر من أشد الأخطار التي تهدد الأمن القومي للدول .

ويقصد بالأمن القومي للدولة : تأمين كيان الدولة ضد أي تهديدات من الداخل أو الخارج وتأمين مصالحها وخلق أنسب الظروف للاستغلال الأمثل للموارد المتاحة لتحقيق الغايات، وهو مثل الأمن العام في ألدولة يعد عنوان تحضرها والمعيار الذي يقاس به إيمانها بالحرية والعدالة والكرامة، ولذلك توليه الدولة جل اهتمامها بعد أن أدركت أن رخاءها واستقرار أوضاعها السياسية والاقتصادية قد أضحى رهيناً باستقرار أمنها وانتشار السكينة في أرجائها[1].

وتنقسم الجرائم التي تستهدف الأمن القومي للدولة إلى قسمين منها جرائم تستهدف أمن الدولة من الداخل والأخرى تستهدف أمن الدولة من الخارج.

ويواجه الأمن القومي في العديد من دول العالم تحديات جديدة في ظل التطورات الاقتصادية والاجتماعية، وانتشار وسائل الاتصال السريع، وخاصة الاتصالات الإلكترونية والتي جعلت المجتمع مجتمعا واحداً مرتبطاً فيما بينه إلكترونيا، مما ساهم في تكوين ثقافة عالمية، واقتصاد عالمي، ومجتمع عالمي، وأصبح من السهل في ظل ذلك التقدم اختراق الحدود فيما بين الدول بعد أن تغير مفهوم الحدود التقليدية المعروفة بالحدود الجغرافية في عصر المعلومات التي أصبح تبادلها وانتقالها تتم بسرعة ويسر،

(1) راجع: فهد سلطان محمد أحمد بن سليمان: مواجهة جرائم الإنترنت دراسة مقارنه، رسالة ماجستير في القانون الجنائي، جامعة القاهرة، كلية الحقوق، 2004، ص74، وراجع أيضا: علي محمد الانسي، ((التأثيرات المختلفة على الأمن القومي اليمني))، مجلة الأكاديمية العسكرية العليا، سنوية،ع 4، سبتمبر 2009،ص12.

حيث يرتبط جهاز حاسوب في بلد ما بشبكة حواسيب في العالم[1]، وقد يرتكب شخص جريمة في بلد يبعد كثيرا عن البلد الآخر باستخدام الحاسوب والشبكة، ومن تلك الجرائم التجسس الإلكتروني [2]، حيث لا يقتصر الخطر- في محاولة اختراق الشبكات والمواقع- على العابثين من مخترقي الأنظمة (HACKERS)، فمخاطر هؤلاء محدودة وتقتصر غالباً علي العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعارة نسخة أخري مخزنة، أما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها أجهزة الاستخبارات للحصول علي أسرار ومعلومات الدول، ومن ثم إفشائها لدول أخري، أو استغلالها بما يضر المصلحة الوطنية للدولة [3].

وبالإضافة إلى جريمة التجسس فإن العصابات الإجرامية أضحت تستخدم الوسائل التكنولوجية الحديثة لتوسيع نشاطها الإجرامي في مجالات الاتجار في المخدرات، وغسيل الأموال، والفساد، والإرهاب، وتجارة البشر والدعارة، وغيرها من الجرائم التي سوف نشير إلى أهمها في هذا المبحث:

([1]) تعتبر المعلومات سمة العصر الذي نعيشه، حيث تكتسب أهميتها من انتشارها، بفضل وجود شبكة المعلومات التي تعد الخلايا العصبية لنقل المعلومات، وقد حملت المعلومات معها آمالا وأحلاما وتوقعات رائعة لخدمة البشرية، إلا أنها مع ذلك قد حملت المخاوف الأمنية وخلقت من المخاطر والمشكلات قدرا مماثلا لتلك الأحلام والآمال والتوقعات، وتعتبر تكنولوجيا المعلومات والاتصال من المفاهيم الحديثة نسبيا، ولا كن استخدامها قد أنتشر بشكل مذهل وسريع، وخاصة الإنترنت، حيث لم تشهد البشرية وسائل للاتصال تتسم بالسرعة والفعالية ، وتؤثر في حياة الناس أينما كانوا اجتماعيا واقتصاديا وثقافيا وتنمويا مثلما فعلت الإنترنت. .راجع: ياسر الصاوي إدارة المعرفة وتكنولوجيا المعلومات، ط1، دار السحاب، القاهرة، 2007،ص47، وص105.

(2) وكأمثله على التجسس على الشركات واختراق حدود الدول والاطلاع على أسرارها:

- اختراق ادوارد أوستن (Edward Austin Singh) البالغ من العمر 23 عاما أنظمة 200 حاسب في دول مختلفة خلال عام 1988م من بينها أنظمة حاسبات تابعه لوزارة الدفاع البريطانية ووكالة ناسا NASA الأمريكية باستخدام بعض تسهيلات النظام المعلوماتي لإحدى الجامعات.
- نجاح الألماني الغربي ماركوس هيس (Marcus Hess)البالغ من العمر 24 عاما في التغلغل بطرق الاتصال ألبعدي في منظومات 30 حاسوب بالولايات المتحدة الأمريكية تتعامل في معلومات عسكرية والحصول منها على معلومات عسكرية وبيانات تتعلق بأبحاث علمية.
- خسرت إحدى الشركات في الولايات المتحدة الأمريكية جميع المناقصات التي دخلتها لعدة شهور حيث رست على شركه منافسة وتبين أن ذلك كان بسبب التجسس على عروض الشركة الخاسرة عن طريق توصيلة سريه بالحاسوب الآلي للشركة.
- قيام بريطاني صغير السن -باستخدام جهاز الكمبيوتر الخاص به - باختراق شبكات المعلومات العسكرية الأمريكية وكشف أدق الاتصالات حيث اعترفت السلطات الأمريكية بأن ذلك الاختراق يعد أشد خطورة.راجع فيما سبق: عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط2، بدون ذكر دار النشر،2000، ص308 وص309. وراجع أيضا: نعيم مغبغب، مخاطر المعلومات والإنترنت- المخاطر على الحياة الخاصة دراسة في القانون المقارن، 1998، ص223.

(3) محمد محمد الألفي، جرائم التجسس والإرهاب الالكتروني عبر الإنترنت، مقال منشور على موقع شبكة النبأ المعلوماتية، الأربعاء 22/فبراير/2006، ت.د 2007/3/5 على الرابط:
http://www.annabaa.org/nbanews/54/273.htm

المطلب الأول

التجسس وإفشاء الأسرار

تعد جريمة التجسس من أخطر الجرائم التي تمس الأمن القومي للدولة نتيجة لما قد يترتب على تلك الجريمة من تعريض مصالح الدولة المختلفة للخطر، والذي قد يؤدي بدوره إلى العدوان عليها من دول أخرى[1]، ومع أن تلك الأنظمة محمية بأنظمة حماية قد تكون متطورة في نظر المؤسسات أو الدول التي تستخدمها، إلا أنها لا تقف حائلا من تلك الاختراقات [2]، وقد زادت عمليات الهجوم على أجهزة الحاسوب في الآونة الأخيرة، ووصل الأمر إلى الأجهزة ذات الطابع السري، في المجال العسكري، ومجال البورصة والبنوك، والتعرف علي حسابات العملاء بل واختراقها في بعض الأحيان، مما ينذر باندلاع حرب قد يطلق عليها مجازا "الحرب الإلكترونية الباردة "[3].

ويتميز الحاسوب بدور كبير في ارتكاب جريمة التجسس وإفشاء الأسرار، نظرا للدخول في عالم الشبكات، والأقمار الصناعية، والبث الفضائي، حيث أصبحت الدول لا تستطيع التحكم في ذلك المجال[4]، وتجاوزت عملية التجسس في اكتشاف ما على الأرض إلى اكتشاف ما بباطنها من مصادر، وفي عصر المعلومات ازدادت حوادث اختراق المراكز العسكرية والإستراتيجية للدول، بتعرضها للقرصنة من أجل الحصول على البيانات والمعلومات المخزنة في ذاكرة الحاسوبات المستخدمة[5]، حيث أصبحت

---

(1) علي محمد الأنسي، مرجع سابق، ص13.

(2) إذا نظرنا إلى حلول أمن المعلومات المطبقة في الأنظمة المعلوماتية والشبكات، التي تعتمدها كثير من الحكومات العربية والإسلامية،مثل جدران النار، ستجدها جميعاً مصنعةً خارجياً، وما يزيد الأمر سوءً هو جهل القائمين على هذه الشبكات العربية التابعة للقطاع الحكومي بهذه الحقيقة، فالاعتماد الكلي على تقنيات أجنبية للحفاظ على أمن معلوماتنا، وتطبيقها على الشبكات الرسمية التابعة للدول العربية والإسلامية، هو تعريض للأمن الوطني والقومي لهذه الدول للخطر، ووضعه تحت سيطرة دول أخرى، بغض النظر عما إذا كانت هذه الدول عدوة أم صديقة، فلقد أصبحت الدول تتجسس على بعضها، بغض النظر عن نوع العلاقات فيما بينها، وهذه حقيقة قائمة، لا يمكن نفيها. وقد تطورت أساليب التجسس في هذا العصر، وأصبحت الأسلحة المعتمدة هي الوسائل إلكترونية وخاصة الإنترنت.

(3) تقرير لشركة مكافي المتخصصة في مجال الحماية الرقمية، موقع شركة الأخبار العربية، ت.د 2008/6/10، على الرابط:

http://www.moheet.com/show_news.aspx?nid=61440&pg=10

(4) أيمن عبد الحفيظ عبد الحميد سليمان: إستراتيجية مكافحة الجرائم ألناشئه عن استخدام الحاسوب الآلي دراسة مقارنة، رسالة دكتوراه في علوم الشرطة، أكاديمية الشرطة، القاهرة،2003، ص131.

(5) ومن تلك القضايا التي تم اختراق أنظمة حساسة، تمكن أحداث لا تتجاوز أعمارهم 15 و 17 عام في ولاية كالفورينا من التسلل عبر شبكة الإنترنت ومن ثم الحصول على ألاف الشفرات الخاصة بالتسلل لمواقع شبكات معلوماتية عن مخبرين أمريكيين يعملان في إطار برنامج الأسلحة النووية، احدهما يطلق عليه مختبر (سامديا) والأخر مختبر(اوك وبدح). راجع عبد الفتاح بيومي حجازي، الأحداث والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2002، ص230..

معلومات الدول عرضة للانتهاك[1]، ولذلك فقد اهتمت التشريعات في جميع الدول بحماية معلوماتها من أن تنتهك أو يتم الاعتداء عليها ،سواء تمثلت تلك المعلومات بمعلومات ذات طابع اقتصادي أو بمعلومات ذات طابع سياسي .

وسوف نتناول في هذا الموضع موقف التشريع اليمني والجزائري من جريمة التجسس وفقا للقواعد القانونية القائمة في كلا التشريعين من خلال بيان أركان الجريمة، ثم نبين مدى إمكانية تطبيقها على التجسس المعلوماتي.

1. أركان جريمة التجسس وإفشاء الأسرار

جريمة التجسس وإفشاء الأسرار مثلها مثل غيرها من الجرائم تتطلب لقيامها توافر الركن الشرعي [2]، والركن المادي، والركن المعنوي.

أ- الركن الشرعي لجريمة التجسس وإفشاء الأسرار

بالعودة إلى النصوص القانونية في القانون اليمني والقانون الجزائري يلاحظ بأنهما قد تضمنا الركن الشرعي لجريمة التجسس وإفشاء الأسرار بمختلف صورها والتي منها الجرائم الماسة باستقلال الجمهورية، و إضعاف القوات المسلحة، وإفشاء سرا من أسرار

---

(1) كشف كتاب صادر في باريس تحت عنوان، عين واشنطن، النقاب عن تورط جهازي المخابرات الأمريكية والإسرائيلية في اختراق جميع أجهزة الكمبيوتر الموجودة في العالم حيث يمكنها التقاط جميع المعلومات المسجلة على تلك الأجهزة، وأكدا مؤلفا الكتاب وهما صحفيان الأول يدعى خابر يزيزو كالفي والثاني تيري بيبيستيه أن إسرائيل أرادت في فترة ألانتفاضه أن تحصل على كافة المعلومات المخزنة في أجهزة الحاسوب الأردنية عن الفلسطينيين فاتفقت مع شركه أمريكية على بيع برنامج معلومات إلى الأردن تستطيع إسرائيل عن طريق ذلك البرنامج أن تتجسس على كل المعلومات الموجودة فيها، وأكد الكاتبان عن وجود ما يسمى بمركز المعلومات الكوني تودع فيه المعلومات التي تم التجسس عليها وتجميعها عن طريق نظم معلوماتية خاصة، تعمل في النهاية لخدمة وكالتي المخابرات الأمريكية والموساد الإسرائيلي، كما يتم التجسس المعلوماتي عن طريق برنامج يتم زراعته من قبل المستفيد في الجهاز المستهدف، ويعرف بالملف اللاصق أو الصامت، وهو ملف باتش Patch صغير الحجم مهمته البقاء بجهاز الضحية، بحيث يمكن عن طريقها السيطرة التامة على الجهاز المستهدف. راجع في اختراق الأجهزة من قبل المخابرات الأمريكية والإسرائيلية، عفيفي كامل عفيفي، مرجع سابق، من ص310الى ص 313، وفي ملفات التجسس راجع: مجلة تكنولوجيا الاتصالات والمعلومات، ع44، فبراير 2005، ص30.

(2) ثار خلاف بين الفقهاء حول مدى اعتبار الركن الشرعي أحد أركان الجريمة، مابين معارض ومؤيد، فبينما يرى أصحاب الاتجاه المعارض: بأن النص القانوني هو عامل ردع، أو شرط أساسي للجريمة، ولا يعد أحد أركانها، لأنه هو الذي يخلقها وليس من الصواب بأن من يخلق يعد جزء ممن يخلقه، ومن ناحية أخرى فانه إذا ما اعتبر النص القانوني ركن في الجريمة فينبغي إحاطة الجاني به، ويترتب على ذلك انتفاء الجريمة في حالة عدم العلم به، بينما يرى أصحاب الاتجاه المؤيد: بان الركن الشرعي يعد أحد أركان الجريمة، إذ لاجريمة بدون نص، وهذا الرأي يعد الصواب من وجهة نظرنا بدليل أن أي ظاهره أو فعل لا يكون مجرما بنص قانوني يعد فعل مباح، ولايمكن العقاب عليه، وبالنظر كذلك إلى الخلاف الفقهي والقضائي حول مدى خضوع جرائم المعلوماتية وخاصة المستحدثة منها للنصوص التقليدية، بحيث يجعلها البعض خارج نطاق التجريم ليؤكد بأن النص القانوني يعد أحد أركان الجريمة، وأن القول بعدم معرفة الجاني للنص ينفي قيام الجريمة وفقا للرأي الأول يتعارض مع القاعدة المعروفة" لايعذر من يدعي الجهل بالقانون". لمزيد من التفصيل راجع: أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديون الوطني للأشغال التربوية، الجزائر، 2002، ص47، وص48.

الدفاع عن البلاد، و التخابر مع دولة أجنبية، حيث نص القانون اليمني عليها في عدد من المواد منها (125، 126، 128).

فنصت المادة (125) على أن: (يعاقب بالإعدام كل من ارتكب فعلا بقصد المساس باستقلال الجمهورية أو وحدتها أو سلامة أراضيها، ويجوز الحكم بمصادرة كل أو بعض أمواله)[1].

ونصت المادة(126) على أن (يعاقب بالإعدام كل من تعمد ارتكاب فعل بقصد إضعاف القوات المسلحة بان:-

- خرب، أو أتلف، أو عيب، أو عطل أحد المواقع، أو القواعد، أو المنشآت العسكرية، أو المصانع، أو البواخر، أو الطائرات، أو طرق المواصلات، أو وسائل النقل، أو المرافق، أو الذخائر، أو المؤن، أو الأدوية، أو غير ذلك مما أعد للدفاع عن البلاد، أو مما يستعمل في ذلك، أو أساء صنعها، أو إصلاحها، أو جعلها غير صالحة ولو مؤقتا للانتفاع بها فيما أعدت له، أو أن ينشأ عنها ضرر.
- أذاع أخبار، أو بيانات، أو إشاعات كاذبة أو مغرضة، أو عمد إلى دعاية مثيرة، وكان من شأن ذلك كله إلحاق الضرر بالاستعدادات الحربية للدفاع عن البلاد، أو العمليات الحربية للقوات المسلحة، أو إثارة الفزع بين الناس، أو إضعاف الروح المعنوية في الشعب) [2].

كما نصت المادة (128) على أن (يعاقب بالإعدام :-

- كل من سعى لدى دولة أجنبية أو أحد ممن يعملون لمصلحتها، أو تخابر معها أو معه، وكان من شأن ذلك الإضرار بمركز الجمهورية الحربي، أو السياسي، أو الدبلوماسي، أو الاقتصادي [3].
- كل من سلم دولة أجنبية، أو أحد ممن يعملون لمصلحتها – بأية صوره كانت وبأية وسيلة أخبار، أو معلومات، أو أشياء، أو مكاتبات، أو وثائق، أو خرائط، أو رسوما،

(1)راجع: المادة (137) من ق.ج.ع.ي، رقم 12 لسنة 1994. ج.ر. ع 3/19، لسنة 1994.

(2)المادة (126) من ق.ج.ع.ي.

(3) المادة (128) من ق.ج.ع.ي. وتمثل المعلومات محل التجسس الاقتصادي أهمية بالغة للدول المتنافسة حربيا بالدرجة الأولى، إلا أن الأمر قد يتعدى ذلك إلى الدول المتنافسة تجاريا، وبهذا الخصوص فقد تمكنت وكالة المخابرات الأمريكية CIA ، ووكالة التحقيقات الفدرالية FBI من القبض على عملاء فرنسيين بعد اتهامهم بالتجسس على إحدى كبريات الشركات الأمريكية في مجال الحاسوب. لمزيد من التفصيل راجع هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق. ص.139

أو صورا، أو غير ذلك، مما يكون خاصا بالمصالح الحكومية، أو الهيئات العامة، أو المؤسسات ذات النفع العام، وصدر أمراً من الجهة المختصة بحضر نشره أو إذاعته.

- كل من سلم دولة أجنبية أو أحد ممن يعملون لمصلحتها، أو أفشى إليها، أو إليه، بأية وسيلة،سراً من أسرار الدفاع عن البلاد، أو توصل بأي طريقة للحصول على سر من هذه الأسرار، بقصد تسليمه أو إفشائه لدولة أجنبية، أو لأحد ممن يعملون لمصلحتها، وكذلك كل من أتلف لمصلحة دولة شيئا يعتبر سرا من أسرار الدفاع أو جعله غير صالح لأن ينتفع به)[1].

وتضمنت المادة(121) تفصيلا لما يعد من أسرار البلاد.[2].

بينما نص القانون الجزائري على جريمة التجسس وإفشاء الأسرار في المواد (من 61 إلى 65) [3].

فنصت المادة (61) على جريمة التخابر مع دوله أجنبية بقولها (يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم بأحد الأعمال الآتية:1-.......... 2- القيام بالتخابر مع دوله أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر أو تقديم الوسائل اللازمة لذلك سواء بتسهيل دخول القوات الأجنبية إلى الأرض الجزائرية، او بزعزعة ولاء القوات البرية أو البحرية أو الجوية أو بأية طريقة أخرى 3- ..). [4].

---

(1) المادة (128) ع.ي.رقم (12) لسنة 1994.

(2) تضمنت المادة (121) من ق.ج.ع.ي حصرا لما يعد من أسرار الدفاع وهي :

- المعلومات الدفاعية والسياسية والدبلوماسية والاقتصادية والصناعية التي تقتضي طبيعتها ألا يعلمها إلا الأشخاص الذين لهم تعلق بذلك، ويجب مراعاة لمصلحة البلاد أن تبقى سرا على من عدى هؤلاء الأشخاص.
- المكاتب والمحررات والرسوم والخرائط والتصميمات والصور وغيرها من الأشياء التي يجب لمصلحة البلاد ألا يعلم بها إلا من يناط بهم حفظها أو استعمالها، والتي يجب أن تبقى سرا على من عداهم، خشية أن تؤدي إلى إفشاء معلومات مما أشير إليه في الفقرة السابقة.
- الأخبار والمعلومات المتعلقة بالقوات المسلحة، وتشكيلاتها، وتحركاتها، وعتادها، وتموينها، وأفرادها، وبصفة عامة كل ماله مساس بالشؤون العسكرية والخطط الإستراتيجية، ولم يكن قد صدر أمر كتابي من السلطة المخول لها ذلك في القوات المسلحة بنشره أو إذاعته .
- الأخبار والمعلومات المتعلقة بالتدابير، والإجراءات التي تتخذ للكشف عن الجرائم المنصوص عليها في هذا الباب من القانون، أو تحقيقها أو محاكمة مرتكبيها، ومع ذلك يجوز للمحكمة التي تتولى ألمحاكمه أن تأذن بإذاعة ما تراه منها.

(3) تضمنت جريمة التجسس وإفشاء الأسرار في ق.ع.ج المواد من (61 إلى 65) من القسم الأول والثاني من الفصل الأول من الباب الثاني المخصص للجنايات والجنح ضد أمن الدولة.

(4) راجع المادة (61) من (القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006المُعدّل والمُتمِّم لقانون العقوبات (ج.ر 84،24 ديسمبر 2006، ص19).

ونصت المادة (62) على : (يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري وكل عسكري أو بحار في خدمة الجزائر يقوم في وقت الحرب مع الجزائر:

1-.......2- القيام بالتخابر مع دولة أجنبية أو مع احد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر)[1].

كما نصت المادة (62) على جريمة إضعاف الروح المعنوية للجيش بقولها (يرتكب جريمة الخيانة ويعاقب بالإعدام كل جزائري يقوم وقت الحرب بأحد الأعمال الآتية: 1-....... 4- المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الغرض منه الإضرار بالدفاع الوطني مع علمه بذلك)[2].

ونصت على جريمة انتهاك أسرار الدفاع المادة (63) حيث ورد النص: (يكون مرتكبا للخيانة ويعاقب بالإعدام كل جزائري يقوم:

- تسليم معلومات، أو مستندات، أو تصميمات، يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة وبأية وسيلة كانت.
- الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات والأشياء والمستندات والتصميمات بقصد تسليمها إلى دولة أجنبية أو أحد عملائها.
- إتلاف مثل هذه المعلومات والأشياء والمستندات والتصميمات بقصد معاونة دولة أجنبية أو ترك الغير يتلفها)[3].

ولم يكتفِ ق.ع.ج على النصوص السابقة الخاصة بتجريم التجسس والتخابر ضد الجزائر ومؤسساتها الدفاعية، بل أنه قد جرم عدداً من الأفعال التي تمس الدفاع، أو الاقتصاد الوطني، سنكتفي بالإشارة إلى ما يتعلق بجمع المعلومات، أو الأشياء، أو الوثائق، أو التصميمات بغرض تسليمها إلى دولة أجنبية ، بسبب أن جمع تلك المعلومات واستغلالها سوف يترتب عليه الإضرار بالدفاع والاقتصاد الوطني [4]، فهذه الجريمة هي التي يمكن إدخالها ضمن جرائم التجسس وإفشاء الأسرار، أما باقي الأفعال التي وردت

---

(1)المادة (62) من الأمر رقم (66-156) المؤرخ في 8 يونيو 1966 يتضمن قانون العقوبات.
(2) راجع الفقرة الرابعة من المادة (62) من الأمر رقم (66-156) المؤرخ في 8 يونيو 1966 يتضمن قانون العقوبات.
(3)المادة (63) من الأمر رقم (75-47)المؤرخ في 17يونيو 1975) المتمم لقانون العقوبات الجزائري .
(4) المادة (65) من نفس الامر السابق.

في نصوص المواد: من (66 إلى 75) فهي وإن كانت تتعلق بكشف معلومات أو إفشاء أسرار إلا أن المشرع الجزائري قد أخرجها من جرائم التجسس وإفشاء الأسرار باعتبار أنها ناتجة عن خطأ، سواء ارتكبت الجريمة من مختص، أم من مؤتمن علي معلومات، وأشياء، ومستندات، وتصميمات يجب أن تحفظ تحت ستار السرية لمصلحة الدفاع الوطني، أم من آخرين استحوذوا على معلومات ، أو أشياء، أو مستندات، أو تصميمات يجب أن تحفظ في إطار السرية لمصلحة الدفاع الوطني، أو يمكن أن تؤدي معرفتها إلى الكشف عن سر من أسرار الدفاع الوطني، أو قاموا بإتلافها واختلاسها، أو إبلاغها إلى علم شخص لا صفة له بها، أو تسليم اختراع أو معلومات تهم الدفاع الوطني بغير إذن سابق من السلطة المختصة ، إلى شخص يعمل لحساب دولة أو مؤسسة أجنبية، إلى غير ذلك من الأفعال التي ترتكب بدون نية الخيانة والتجسس[1].

من خلال النصوص السابقة يلاحظ عدم تضمين ق.ج.ع.ي نصوص قانونية تجرم التجسس الرقمي بشكل واضح من خلال تضمينه عبارات يدخل فيها مفهوم التجسس الرقمي، واكتفى بالنص على جريمة التجسس ضمن الجرائم التقليدية المتعلقة بأمن الدولة[2]، بخلاف القانون الجزائري الذي تناول الجريمة من خلال نصوص تقليدية ونصوص مستحثه تتناسب مع جريمة التجسس المعلوماتي.

كما يلاحظ بأن المشرع الجزائري قد فرق بين نوعين من الجرائم الماسة بأمن الدولة، النوع الأول: جرائم عمدية وهي جرائم الخيانة والتجسس، إذ يجب أن يتوفر القصد الجنائي لاقترافها، والنوع الثاني وهي الجرائم التي وإن تم من خلالها كشف أسرار، أو تسليم معلومات، أو إتلافها وتخص الدفاع والاقتصاد الوطني، إلا أن هذا النوع من الجرائم هي جرائم غير عمدية يشترط المشرع فيها عدم توفر نية الخيانة والتجسس، وبالتالي فإن عقوبتها أخف من عقوبة جرائم الخيانة والتجسس فعقوبتها السجن وليس الإعدام، وكذلك فعل المشرع اليمني.

وقد وجد خلاف حول المعيار الذي يتم التفرقة بواسطته بين الخيانة والتجسس[3]

---

(1)راجع : المواد من (66 إلى 75) من الأمر رقم (75-47) المؤرخ في 17يونيو 1975 المتمم لقانون العقوبات الجزائري.

(2)المواد من (125 إلى 128) من قانون العقوبات اليمني رقم (12) لعام 1994.

(3) محمد صبحي نجم، شرح قانون العقوبات الجزائري –القسم الخاص، ط5، ديوان المطبوعات الجامعية،2004، ص191

اعتمد **الأول** للتفرقة بينهما على ضابط أو معيار موضوعي، فعندما يقوم المتهم بتسليم الغير معلومات أو أشياء أو أسرار تتعلق بأمن وسيادة واستقلال الدولة نكون بصدد خيانة، فالخيانة تعني التسليم، أما التجسس فيقوم بمجرد البحث وجمع المعلومات والتخابر.

ونلاحظ من جهة ثانية اعتماد معيار الباعث من ارتكاب الجريمة للتفرقة بين الأمرين فإذا كان الباعث هو العداء للدولة، فإن الفعل يكون خيانة وإذا كان الباعث يتمثل بالطمع والحصول على المال فإن الفعل هو التجسس.

ومن جهة أخرى الاعتماد على جنسية مرتكب الجريمة فإذا كان المتهم ينتمي إلى الدولة التي ارتكبت الجريمة ضدها فتكون جريمة خيانة، وإذا كان ينتمي إلى دولة أخرى فإنه يكون مرتكبا لجريمة تجسس، فالخيانة تكون من الوطني، والتجسس يكون من الأجنبي، ولقد اشترط المشرع الجزائري في الخيانة أن يكون الجاني جزائريا، أو عسكريا يخدم في الجيش الجزائري، أو في البحرية الجزائرية، بينما تطلب في التجسس أن يكون الجاني أجنبياً وفق نص المادة (64) [1].

ونظرا لخطورة تلك الجرائم فلم يكتفِ المشرع الجزائري بتجريمها بتلك النصوص، بل نص عليها وشدد من عقوبتها ضمن عقوبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب تعديل قانون العقوبات نوفمبر 2004، فبعد أن جرم جريمة الدخول والبقاء في صورتها المجردة، نص على تشديد العقوبة إذا كانت تلك الأفعال موجهة ضد مؤسسات الدفاع الوطني والهيئات التابعة لأشخاص القانون العام (مادة 349 مكرر3).

ب- الركن المادي لجريمة التجسس وإفشاء الأسرار

يقوم الركن المادي في جريمة التجسس وإفشاء الأسرار وفقا لنصوص القانون اليمني على سلوك إجرامي مادي، فلم يتضمن القانون في نصوصه ما يدل من قريب أو بعيد على اقتراف الجريمة بسلوك تقني معلوماتي، بخلاف القانون الجزائري الذي

(1) محمد صبحي نجم، مرجع سابق، ص191.

تضـمن جريمـة التجسـس الإلكترونيـة ضـمن جـرائم المسـاس بأنظمـة المعالجـة الآليـة للمعطيات حيث شدد من عقوبة تلك الجرائم إذا استهدفت الدفاع الوطني[1].

وتختلف الأفعال التـي تقتـرف بهـا الجريمـة مـن صـورة إلـى أخـرى، ففـي جريمـة المساس بسلامة الجمهورية لم يحدد المشرع السلوك أو الأفعال التي يمكن أن ترتكب بها الجريمة، وبالتالي فإن أي فعل يؤدي إلى المساس باستقلال الجمهورية أو وحدتها أو سلامة أراضيها تقوم به الجريمة.

وفي جريمة إضعاف القوات المسلحة، أو إفشاء أسرار الدفاع، أو التخابر مع دولـة أجنبية، فإن الأفعال التي تقوم بها الجريمة هي إذاعة أخبار، أو بيانات، أو إشاعات كاذبة أو مغرضـة أو دعايـات مثيـرة، إذا مـا كـان مـن شـأن تلـك الأفعـال إلحـاق الضـرر بالاستعدادات الحربية للدفاع عن البلاد، أو العمليات الحربية للقوات المسلحة أو إثارة الفزع بين الناس، أو إضعاف الروح المعنوية في الشعب، كما أن من تلك الأفعال التي تتحقق بها الجريمة إشاعة المعلومات التي تهول من العدو وعتاده وتهون من الجيش اليمني أو الجزائري.

وفي صورة الجريمة المتمثلة في التخابر مع دولة أجنبية، أو إفشاء أسرار البلاد فإن الأفعال التي تقوم بها الجريمة هي فعلي الإفشاء والتخابر، الإفشاء لأي سر من أسرار البلاد الاقتصادية، أو السياسية، أو العسكرية، والتخابر مع دولة أجنبية، أو مع احد ممن يعملون لصالحها، وكان من شأن ذلك إلحاق الضرر بمركز الجمهورية الحربي أو السياسي أو الدبلوماسي أو الاقتصادي، فكل من سعي بالاتصال بدولة أجنبية بغرض تقديم أسرارا من شأنها أن تؤثر على دولتي اليمن أو الجزائر وقد تؤدي إلى القيام بأعمال عدوانية ضد أي منهما فإنه يكون مرتكبا لجريمة التجسس وإفشاء الأسرار.

كما أن الجريمة تقوم بفعل التسليم لدولة أجنبية أو أحد ممن يعملون لصالحها معلومات، أو أشياء، أو مكاتبات، أو وثائق، أو خرائط، أو رسومات، أو غير ذلك مما يعد محظوراً نشره، ويكون خاصا بالمصالح الحكومية، أو الهيئات والمؤسسات ذات النفع العام، ولم يكتف المشرع بتجريم فعل التسليم أو الإفشاء بل إنه قد جرم الأفعال التي

(1) راجع: المادة (394 مكرر3) من القانون رقم (04 - 15) المؤرخ في 10 نوفمبر2004 المعدل والمتمم لقانون العقوبات (ج.ر 71ص11).

تسبقهما، ومنها فعل التوصل بأي طريقة إلى الأسرار بهدف إفشائها، ويكون المشرع بذلك قد أراد أن يحمي تلك الأسرار قبل أن تذاع وتسلم للآخرين .

و جريمة انتهاك أسرار الدفاع الوطني تشمل جميع الأسرار التي لها علاقة بالدفاع أو الاقتصاد الوطني[1]، فكل معلومة مما يحضر القانون تداولها ويكون لها قيمة دفاعية أو اقتصادية في سوق المعلومات يعد الإفشاء عنها أو كشفها لمن ليس له الحق في الإطلاع عليها جريمة.

وتتحقق الجريمة كذلك بتسليم ونقل الحيازة لمحل السر إلى دولة أجنبية أو أحد عملائها، كما تتحقق بقيام الجاني بالإطلاع على السر الذي لم يكن من حقه الإطلاع عليه والاستحواذ عليه بقصد تسليمه لدولة أجنبية أو لأحد عملائها، وتعد الجريمة قائمة في حق الجاني بمجرد الاستحواذ على محل السر ولو لم يقم بتسليمه طالما كان القصد من الاستحواذ هو تسليم ذلك السر لدولة أجنبية ،أو لأحد عملائها، ولا يهم بعد ذلك إن كان المتهم يفهم مضمون محل السر أم لا.

كما تعد الجريمة قائمة في حالة قيام الجاني بإتلاف السر، وإتلاف السر لا يتم إلا بإتلاف الوعاء المادي الذي يحويه كتمزيق ورقة كتب بها [2]، ويعاقب كذلك على إتلاف المعلومات بطريقة مستقلة عن كيانها المادي.[3].

وجريمة إتلاف المعلومات اعتبرت وفقا لنص هذه المادة من جرائم التجسس لكونها تستهدف إتلاف المعلومات التي تم الاتفاق أو التخابر بشأنها بين مرتكب الجريمة وبين دولة أخرى أو شخص أو جهة يعملوا لصالحها.

---

(1) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضة العربية،2004، ص 281.

(2) راجع محمد صبحي نجم، مرجع سابق، ص191.

(3) نتج عن التقدم التكنولوجي وثورة المعلومات والتقنية تقدما هائلا في تخزين الكم الهائل من المعلومات، إلا أنها بنفس الوقت قد أتاحت للمجرمين المستخدمين للتقنية الحديثة ارتكاب العديد من الجرائم المعلوماتية ،ومنها إتلاف المعطيات المخزنة في جهاز الحاسوب، حيث تعتبرها بعض القوانين من جرائم التجسس إذا تعلقت بمعطيات هامة تخص الدفاع أو الاقتصاد الوطني، وإذا كان لا يمكن تطبيق القانون التقليدي على هذه الجرائم دون التأثير على الوعاء الذي خزنت به وفقا للرأي القائل بأن إتلاف المعطيات يشترط فيه إتلاف الوعاء الذي تحويه، فإن ذلك لا يثير أي إشكال في الدول التي نصت قوانينها على تجريم التجسس المعلوماتي، بينما تثار المشكلة في الدول التي لم تسن تشريعات لمواجهة الإجرام المعلوماتي مما يتطلب تضمين القوانين الحديثة نصوص قانونية لمواجهة جريمة التجسس المعلوماتي، ومع ذلك فإن هذا الرأي منتقد نظرا لأهمية المعطيات مستقلة عن الوعاء الذي تحويه، فالمستهدف من جريمة التجسس هي المعطيات وليس الوعاء، وعلية فلا نرى مانعا من تطبيق القوانين التقليدية على إتلاف المعطيات الهامة التي تدخل في إطار جريمة التجسس وفقا لنصوص القوانين التي لم تحدد وسيلة أو طريقة بعينها لاقتراف الجريمة ومنها القانون اليمني والجزائري.

ج- الركن المعنوي

يتوافر الركن المعنوي لجريمة التجسس وإفشاء الأسرار إذا توافر القصد الجنائي العام بعنصريه: العلم والإرادة، بالإضافة إلى تطلب القصد الجنائي الخاص.

وتعد هذه الجريمة من الجرائم العمدية، إذ يجب أن يتحقق فيها القصد الجنائي العام بعنصرية العلم والإرادة حتى يمكن القول بقيامها، فيجب أن يكون الجاني عالما وقت ارتكابه للجريمة بكافة العناصر المكونة لها، ويجب أن يكون عالما بأنه يقوم بفعل من شأنه أن يتسبب في إفشاء الأسرار المتعلقة بالدولة أو إحدى هيئاتها أو مؤسساتها العمومية.

ويجب كذلك أن يكون عالما بأنه يقوم بفعل من شأنه إعانة العدو، كما يجب أن يكون عالما انه يقدم على فعل من شأنه أن يتسبب في إضعاف الروح المعنوية للجيش.

وتقوم الجريمة إذا قام الجاني بتسليم، أو الاطلاع، أو إتلاف سر من أسرار الدفاع الوطني لمصلحة دولة أجنبية أو أحد عملائها.

كما يجب أن يتوافر بجانب عنصر العلم عنصر الإرادة والتي تتمثل في إرادة تحقيق النتيجة وهي إفشاء تلك الأسرار أو تسليمها للغير، دولة كانت أو فرداً يعمل لصالحها.

و إضافة إلى القصد العام فقد تطلب المشرع اليمني والجزائري توافر القصد الجنائي الخاص في بعض صور جريمة التجسس وإفشاء الأسرار، ومن تلك الجرائم جريمة التخابر مع دولة أجنبية، أو مع احد ممن يعملون لصالحها، وكذلك ارتكاب أي فعل بقصد المساس باستقلال الجمهورية أو وحدتها أو سلامة أراضيها، أو بنية إضعاف القوات المسلحة، فقد تطلب أن يكون من شأن ذلك الإضرار بمركز الجمهورية الحربي أو السياسي أو الدبلوماسي أو الاقتصادي.

فيجب أن تنصرف إرادة الجاني الحرة والمدركة إما إلى تسليم، أو الإطلاع، أو إتلاف سر من أسرار الدفاع الوطني لمصلحة دولة أجنبية، أو أحد عملائها، إضرارا بالدولة وبأسرارها ووسائل دفاعها ومصالحها الوطنية والقومية.

كما يتطلب المشرع الجزائري لقيام جريمة الخيانة والتجسس توفر قصد جنائي خاص لدى الجاني يتمثل في اتجاه إرادته إلى إعانة العدو وقت الحرب.

2- عقوبة جرائم التجسس وإفشاء الأسرار ومدى انطباقها في القانون التقليدي

أ- عقوبة جرائم التجسس

يعاقب المشرع اليمني على جريمة التجسس وإفشاء الأسرار المتعلقة بالأمن القومي للدولة بعقوبة الإعدام(1) سوءً أكانت الجريمة تتمثل بالمساس باستقلال الجمهورية وسلامة أراضيها، أم بارتكاب فعل بقصد إضعاف القوات المسلحة، أم الاتصال مع دولة أجنبية بغرض التخابر أو إفشاء الأسرار، أو تسليمها أو من يعمل لمصلحتها سرا من أسرار الدفاع(2).

ويجوز الحكم بمصادرة كل أو بعض أمواله.

كذلك تكون عقوبة كل من حرض، أو اشترك في اتفاق جنائي لارتكاب إحدى الجرائم المشار إليها، أو شرع في ارتكاب أي منها بذات العقوبة المقررة لها ولو لم يترتب على فعله اثر(3).

وفي القانون الجزائري تكون عقوبة جريمة التجسس والخيانة في أي صورة من صورها –التخابر مع دولة أجنبية، أو إضعاف الروح المعنوية للجيش، أو انتهاك أسرار الدفاع الوطني – هي الإعدام(4).

وقد نص القانون الجزائري على عقوبات أخرى للجريمة إذا ارتكبت بواسطة المعلوماتية وهي السجن والغرامة (5).

---

(1) راجع المواد (من125 إلى 129) من قانون العقوبات اليمني رقم (12 لسنة 1994.

(2) يلاحظ على النصوص الخاصة بجريمة التجسس في القوانين الوطنية بأنها تعاقب على جريمة التجسس عندما تقترف من قبل أفراد أو عصابات إجرامية يقعون تحت قبضتها، حيث كانت تلك الجرائم ترتكب عن طريق عملاء لدول معينة يتم زرعهم في دول أخرى للتجسس عليها، ومع أن تلك الجريمة لازالت ترتكب عن طريق أولئك العملاء سواء بالوسائل التقليدية أم الإلكترونية، فإن المشكلة تكمن حينما ترتكب تلك الجريمة- التجسس السياسي أو العسكري أو التجاري أو الصناعي- بواسطة دول تستخدم فيها أنظمة للتجسس، بل أن التقنيات والبرامج المصدرة للدول الأخرى قد تكون من إنتاجها وبذلك يكون من السهولة التجسس على معلوماتها، وعلى وجه الخصوص الدول العربية والإسلامية، وإذا كان بإمكان الدول سن العقوبات وتطبيقها في حق مرتكبي تلك الجرائم كأفراد، فمن يستطيع سن العقوبات وتطبيقها على تلك الدول وهي الأقوى في شتى المجالات ، وبالتالي فإنه لا يكون أمام الدول العربية والإسلامية ألا أن تتنبه لهذا الأمر وتعد العدة لمواجهة مخاطر التقنية، وقبل هذا يجب عليها أن تعد نفسها لكي تصبح منتجة للتقنية، ومواكبة لها فالحماية في هذا الشأن هي حماية تقنية قبل أن تكون حماية جنائية.

(3) المادة (129) من ق.ع.ي.

(4) راجع: المواد (61، 62، 63) من الأمر رقم (66- 156) المؤرخ في 8 يونيو 1966يتضمن قانون العقوبات المُعَدل والمُتَمم .

(5) راجع المادة (394 مكرر 3) من القانون رقم (04) المؤرخ في 10 نوفمبر 2004المُعَدِل والمُتَمِم لقانون العقوبات.

وبالتـالي فـإن العقوبـة التـي تطبـق فـي حالـة اقتـراف الجريمـة تكـون هـي العقوبـة الأشد(1).

بينما تكون عقوبة السجن المؤبد لكل من يجمع أشياء، أو معلومات، أو وثائق، أو تصميمات تضر بمصالح الدفاع والاقتصاد الوطني بغرض تسليمها إلى دولة أجنبية(2).

وتقتصر العقوبة على السجن المؤقت في حالة أن ترتكب الجريمة بسبب التقصير أو الإهمال، وذلك عندما لا يتوفر قصد الخيانة أو التجسس، حيث تكون من عشر سنوات كحد أدنى إلى عشرين سنة كحد أقصى إذا ارتكبت جريمة إتلاف، أو اختلاس، أو أخذ صورة لمعلومات أو تصميمات يجب أن تحفظ تحت ستار السرية لمصلحة الدفاع الوطني ، أو تم إبلاغها إلى علم شخص لا صفة له بها أو إلى الجمهور وتخص الدفاع الوطني سواء من الأمين على حفظها أم من الغير إذا ترك لهم المجال من قبل الأمين، وتكون العقوبة السجن من خمس سنوات إلى عشر سنوات إذا كان الحارس أو الأمين قد ارتكب الجريمة برعونة أو بغير حيطة أو بعدم تبصر أو إهمال أو بعدم مراعاة الأنظمة.

أما جريمة تسليم اختراع أو معلومات تهم الدفاع الوطني بغير إذن سابق من السلطة المختصة إلى شخص يعمل لحساب دولة أو مؤسسة أجنبية فتكون عقوبتها الحبس من عشر سنوات إلى عشرين سنة(3).

ب- مدى انطباق النصوص التقليدية على جريمة التجسس المعلوماتية

من خلال النصوص الخاصة بجريمة التجسس وإفشاء الأسرار في ق.ج.ع.ي يلاحظ بأنها وإن كانت وقت صدورها إنما صدرت للتعامل مع الجرائم ذات الطابع المادي، حيث توحي تلك النصوص بأنها وضعت للتعامل مع جريمة التجسس بصورتها المادية باستثناء بعض العبارات التي يمكن أن تنصرف إلى الجريمة بصورتها المنطقية، من خلال النص على تحقق الجريمة إذا ما تم اقترافها بأي وسيلة أو طريقة كانت، ونظرا لعدم تضمين المشرع اليمني نصوصاً قانونية تجرم التجسس المعلوماتي بصورة

(1) من المقرر قانونا أنه يجب أن يوصف الفعل الواحد الذي يحتمل عدة أوصاف بالوصف الأشد، ومن ثم فإن القضاء فيما يخالف هذا المبدأ يعد خطأً في تطبيق القانون، ولما كان من الثابت – في قضية الحال- أن محكمة الجنايات وصفت جريمة واحدة بوصفين مختلفين فإنها تكون بقضائها كما فعلت قد خالفت القانون، ومتى كان كذلك استوجب نقض الحكم المطعون فيه. المجلة القضائية93/3،ص 260 مشار إليها لدى: يوسف دلاندة، قانون العقوبات منقح بالتعديلات التي أدخلت عليه بموجب القانون رقم(04- 15) المؤرخ في 10 نوفمبر 2004 ومدعم بأحدث مبادئ واجتهادات المحكمة العليا، دار هومه، الجزائر، 2005، ص25.

(2) المادة (65) من الأمر رقم (75- 47) المؤرخ في 17 يونيو 1975 المتمم لقانون العقوبات.

(3) راجع المواد (66، 67: 68، وما بعدها) من الأمر السابق.

صريحة إزالةً للالتباس، فيمكن تطويع تلك النصوص لكي تنطبق على جريمة التجسس التي ترتكب بواسطة النظم المعلوماتية لعدد من المبررات هي:

1) وردت بعض النصوص المتعلقة بإفشاء الأسرار واسعة من حيث الألفاظ التي تحمل في طياتها التجريم سواء تم ارتكابها من خلال الوسائل التقليدية أم الوسائل الإلكترونية، وسواء تمثلت أفعالها بأفعال مادية محسوسة مثل المكاتبات أو المحررات، أم بصورة نبضات كهرومغناطيسية، فقد توسع المشرع في لفظ الأسرار في نص المادة(121) والمادة(128)ع.ي بحيث شملت عدة صور لما يمكن أن يمثل بحسب طبيعته سرا حتى ولو لم يتمثل في صورته المادية، فبعد أن نص على الأخبار والمعلومات والأشياء أردف ذلك بكلمة المكاتبات بمعنى أن المشرع أشار إلى أن المعلومات قد تتمثل في غير المكاتبات (المحررات)، ولبيان ذلك القصد بصورة أوضح، فقد ذكر في نص المادة(121) عبارة " وغيرها من الأشياء التي يجب لمصلحة البلاد ألا يعلم بها إلا من يناط بهم حفظها أو استعمالها "، كما ذكر في نص المادة (128)" أو غير ذلك مما يكون خاصا بالمصالح الحكومية، أو الهيئات العامة، أو المؤسسات ذات النفع العام" وبالتالي فإن المشرع لم يشترط شكل معين لتلك المعلومات، فلم يشترط الصفة المادية كالمحررات والوثائق كما في الجرائم الأخرى مثل السرقة وغيرها من الجرائم التي اشترط فيها المشرع الصفة المادية (1).

2) إن المشرع اليمني لم يشترط لارتكاب الجريمة أن ترتكب بوسيلة معينة، فقد نصت المادة :(128) على عقوبة كل من سلم دولة أجنبية، أو أحداً ممن يعملون لمصلحتها، أو أفشى إليها، أو إليه بأية وسيلة سرا من أسرار الدفاع ، وبالتالي فإن نصوص القانون اليمني المتعلقة بجريمة التجسس تنطبق على تلك الجريمة سواء تم ارتكابها بالوسائل التقليدية، أم بالوسائل الإلكترونية، وسواء كانت الأفعال التي تمثل الركن المادي لتلك الجريمة أفعالا مادية كالمكاتبات أو الوثائق وغيرها، أم أفعالا غير مادية تتمثل في النبضات الكهرومغناطيسية للمعلومات المخزنة في أجهزة

---

(1)راجع : أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص135.

الحاسوب، فالجاني الذي يقوم بالدخول إلى الشبكة والحصول منها على معلومات أو احتفاظه بها داخل الحاسوب بغرض التجسس يعد مرتكبا للجريمة.

كذلك فإن الجاني الذي يقوم بحيازة وسائط متعددة تحوي معلومات محظوراً إفشاؤها، يعد مرتكبا لجريمة التجسس وإفشاء الأسرار، حيث أن القانون يجرم حيازة تلك المعلومات بذاتها أو تسليمها لدولة أجنبية بغض النظر عن الوسيلة المستخدمة.

ويمكن أن يتحقق نقل الأسرار عن طريق المعالجة الآلية للبيانات وتفريغها إلى دعامات مادية أو أشرطة ممغنطة وتسليمها إلى دولة أجنبية، وتتحقق الجريمة كذلك عن طريق التراسل عبر الشبكات المعلوماتية مثل الإنترنت والبريد الالكتروني والهاتف اللاسلكي[1].

والقانون اليمني بتجريمه للأفعال التي من شأنها أن تؤدي إلى إفشاء أسرار الدولة السياسية أو الاقتصادية، إنما يجرمها بهدف حماية تلك المعلومات من أن تنتهك، فأساس الحماية هي المعلومات بذاتها.

وبالتالي فإنه لا يجرم فعلي الدخول والبقاء بقصد الإطلاع على تلك المعطيات وتسريبها مثل تشريعات بعض الدول ومنها الولايات المتحدة الأمريكية وفرنسا والجزائر وغيرها من الدول التي وفرت نوعين من الحماية لتلك المعطيات.

النوع الأول: يتمثل في تجريم فعل الدخول أو البقاء بغض النظر عن النتيجة أو الغرض منهما ومن ذلك التشريع الفرنسي وعلى نفس السياق التشريع الجزائري.

والنوع الثاني: يتمثل في توفير الحماية إذا استهدف الدخول معطيات بعينها تكون مخزنة في الأنظمة المعلوماتية لأجهزة المؤسسات أو الهيئات العامة ومن ذلك التشريع الأمريكي.

لما تم ذكره فإن على المشرع اليمني أن يجرم فعل الدخول أو البقاء، ويشدد العقوبة في حالة أن تستهدف تلك الأفعال المعطيات الحساسة والمخزنة بالأجهزة الحكومية وعلى وجه الخصوص المخزنة في أجهزة مؤسسات الدفاع الوطني أسوة

(1) أحمد خليفة الملط، مرجع سابق، ص337.

بغيره من التشريعات التي نصت على جريمة التجسس في مجال المعلوماتية، ومنها التشريع السعودي والتشريع الإماراتي[1] .

كذلك فإنه من خلال النصوص القانونية المتعلقة بجريمة التجسس في القانون الجزائري يمكن الخروج بإمكانية تطبيقها على جريمة التجسس التي ترتكب بواسطة النظم المعلوماتية، نظرا لكون تلك النصوص لم تحدد طريقة بعينها ،أو وسيلة لاقترافها مما يتيح المجال لتطبيقها على جريمة التجسس المعلوماتي.

فتقوم الجريمة باختراق الأنظمة المعلوماتية التي تخزن فيها المعلومات المتعلقة بالدفاع الوطني أو الاقتصاد بغرض تسليمها للغير بعد نقلها وتخزينها في وعاء مادي، أو قيامه بتسليمها عن طريق إرسالها بالبريد الالكتروني، أو تسليمها بعد أن يقوم بطباعتها أو بأية وسيلة كانت طالما أن الجريمة قامت على اختراق نظام معلوماتي واستهدفت من خلاله المعلومات ذات الطبيعة السرية والمتعلقة بالأمن القومي للدولة ،وقيامه بتسليمها لدولة أجنبية أو لأحد عملائها .

فمثلما يتم التسليم المادي للمعلومات بشكل مكتوب، أو بصورة وثائق أو خلاف ذلك، فإنه يمكن أن يتم التسليم معنويا بقيام الجاني بتسليم المعلومات عن طريق نقلها من

---

(1) نصت الفقرة (2) من المادة السابعة من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/17) المؤرخ في8/ 3/ 1428هـ، بناء على قرار مجلس الوزراء رقم (79) المؤرخ في 1428/3/7هـ الموافق 26/ 3/ 2007 صراحة على تجريم التجسس المعلوماتي بقولها (يعاقب بالسجن مدة لا تزيد عن عشر سنوات وبغرامة لا تزيد عن خمسة ملايين ريال سعودي، أو بإحدى هاتين العقوبتين، لكل شخص يرتكب أيا من الجرائم المعلوماتية ألآتية:1 .... 2- الدخول غير المشروع إلى موقع الكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو احد أجهزة الحاسوب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني). وتنص المادة (22) من القانون الاتحادي الإماراتي رقم(2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على: (يعاقب بالسجن كل من دخل بغير وجه حق موقعاً أو نظاماً مباشرة، أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الحصول على بيانات، أو معلومات حكومية سرية إما بطبيعتها، أو بمقتضى تعليمات صادرة بذلك، فإذا ترتب على الدخول إلغاء تلك البيانات، أو المعلومات، أو إتلافها، أو تدميرها، أو نشرها، تكون العقوبة السجن مدة لا تقل عن خمس سنوات، ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى، والتجارية، والاقتصادية).

راجع نظام مكافحة الجرائم المعلوماتية السعودي على موقع جوروسيديا، والموقع السوري للاستشارات والدراسات القانونية، وموقع صحيفة الوطن،ع 2674 ،الجمعة 16 محرم 1429 الموافق 25يناير 2008، و تم التأكد من أن البيانات مازالت متاحة في 2009/9/4 على الروابط:

http://ar.jurispedia.org/index.php/%D9%86%D8%B8%D8%A7%D9%85_%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9_%D8%AC%D8%B1%D8%A7%D8%A6%D9%85_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9_(sa)

http://www.barasy.com/forum/showthread.php?t=1846

http://www.alwatan.com.sa/news/newsdetail.asp?issueno=2674&id=39019&groupID=0

وراجع في القانون الإماراتي موقع الشبكة العربية لمعلومات، ت.د 2006/12/2 على لرابط:

http://www.openarab.net/laws/2006/laws8.shtml

جهاز الحاسوب الذي تم اختراقه أو الجهاز الذي يعمل الجاني عليه إلى جهاز دولة أخرى أو أحد عملائها، أو بواسطة برامج يتم من خلالها اختراق أجهزة الحاسوب المستهدفة .

وبالعودة إلى نصوص مواد قانون العقوبات الجزائري ومنها المادة(61) الفقرة (2)، والمادة (63) الفقرة(1)، يلاحظ بان جريمة تسليم المعلومات للعدو تتحقق متى تم التسليم بأي صورة أو وسيلة كانت.

وبالإضافة إلى إمكان تحقق جريمة التجسس بفعل التسليم، أو الاطلاع، فإن بالإمكان تحققها بفعل الإتلاف، الذي من خلاله يقوم الجاني بالدخول إلى النظام المعلوماتي المخزن فيه المعلومات ومن ثم العمل على تدمير النظام بهدف تدمير وإتلاف المعلومات، أو إتلاف المعلومات بدون أن يتأثر النظام، ففي هذه الحالة يقوم الجاني بالتجسس على المعلومات بغرض إتلافها حتى لا تتحقق الاستفادة منها من قبل الدولة.

ويلاحظ بأن قانون العقوبات الجزائري لم يقتصر على العقوبات التقليدية لجريمة التجسس بل أنه قد ساير التشريعات الحديثة ومنها التشريع الفرنسي، وأستحدث نصوصاً قانونية لمواجهة الإجرام المعلوماتي [(1)]،ومنها جريمة الدخول إلى نظام المعالجة الآلية للمعطيات، وجريمة إتلاف المعطيات التي يتضمنها النظام، إضافة إلى جريمة حيازة أو إفشاء المعطيات المتحصل عليها من جرائم الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، ولم يقتصر المشرع الجزائري على ذلك فحسب بل إنه خصص مادة قانونية تنص على مضاعفة العقوبات الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام[(2)]، مما يوحي بصورة صريحة أن تلك النصوص تنطبق على جريمة التجسس التي تستهدف فيها المعلومات ذات الطابع السري الموجودة في أنظمة المعالجة الآلية للمعطيات أوفي أوعية تخزين، و ذلك مشروط بدون الإخلال بتطبيق عقوبات أشد.

---

(1) المواد من(394 مكرر إلى 394مكرر 7) من القسم السابع من ق.ع.ج رقم(04-15 المؤرخ في10 نوفمبر 2004م) المُعَدِلْ والمُتَمِمْ للأمر رقم (66-)156 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو سنة 1966 المتضمن قانون العقوبات.

(2) المادة(394 مكرر3) من القانون رقم(04-15) المؤرخ في10 نوفمبر 2004م المُعَدِلْ والمُتَمِمْ لقانون العقوبات.

المطلب الثاني

غــــسيـل الأمـــــوال

تعد ظاهرة غسيل الأموال ظـاهرة قديمـة، حيث تشير دراسـات تاريخيـة إلـى أن من قام بغسل الأموال هم رجال العصابات القديمة في الصين، فقد كانت التجارة والقوافل التجاريـة والأربـاح الناتجـة عنهـا تستخدم كوسيلة لإخفـاء أمـوال الجريمـة خاصـة جـرائم السطو والاستيلاء على أموال الفلاحين.

وظهرت جريمة غسيل الأموال لأول مرة في الولايـات المتحدة الأمريكيـة خـلال الفتـرة مـن 1920 إلـى 1930، حيـث لجـأت عصـابات المافيـا إلـى إنشـاء محل لغسـيل الملابس من أجل استثمار الأموال التي تحصلت عليها بطريقة غير مشروعة من تجـارة المخدرات، بهدف إخفاء أصل تلك الأموال، حيث كانت تضم الدخل الناشئ عن استخدام المخـدرات إلـى الإيـرادات اليوميـة للمغاسـل، وبالتـالي يخضـع هـذا الـدخل مـع الإيـرادات للضـرائب، فكمـا يتم غسل الملابس غير النظيفة لتصبح صـالحة للاستخدام، فـإن الأمـوال ذات الأصول الإجرامية تغسل وتصبح نظيفة وصـالحة للتداول الاقتصـادي والمـالي دون عوائق[1]، وفـي نهايـة القرن العشرين بـرزت ظـاهرة غسيل الأمـوال لتشكل تحـديا للـنظم الاقتصـادية والقانونية القائمة، وتعود الأسباب إلى اتساع دائرة المدفوعات الافتراضـية[2]

---

(1) راجع:عبد الفتاح سليمان، مكافحة غسل الأموال، دار الكتب القانونية، القاهرة،2005 ، ص 7. وراجع أيضا: محمد حافظ رهوان، ((عملية غسيل الأموال،مفهومها ،خطورتها وإستراتيجية مكافحتها))، مجلة الأمن والقانون، أكاديمية شرطة دبي،ع2، يوليو 2002،ص127.

(2)أصبح انتقال رؤوس الأموال عبر الدول أكثر يسرا في ظل تدويل الاقتصاد العالمي، ونمو أسواق المال الدولية وقد حمل هذا في طياته تنامي حركة الجريمة الاقتصادية المنظمة وتزايد حركة تداول أموال المنظمات الإجرامية على المستوى الدولي والمحلي بهدف تغيير صفة الأموال التي يتم الحصول عليها بطرق غير مشروعة وإعادة تدويرها في مجالات وقنوات استثمار شرعية لكي تبدو كما لو كانت قد تولدت من مصدر مشروع، لذلك تزايد الاتجاه – في السنوات الأخيرة – نحو مكافحة عمليات غسل الأموال القذرة من خلال جهود دولية ووطنية حثيثة استهدفت الحد من تلك الظاهرة، والحيلولة دون نموها، لما لذلك من آثار بالغة على استقرار أسواق المال الدولية، بل على الاستقرار الاقتصادي والاجتماعي على كافة المستويات ويتفق هذا التوجه مع قاعدة اقتصادية هامة مفادها أن رؤوس الأموال القلقة الباحثة عن الشرعية لا تبني اقتصادا ولا تحقق تنمية اقتصادية حقيقية، حيث لا يهتم غاسلو الأموال بالجدوى الاقتصادية للاستثمار قدر اهتمامهم بالتوظيف الذي يسمح بإعادة تدوير تلك الأموال في أشكال عديدة وعبر فترات زمنية متلاحقة، وهو ما يتناقض مع كل القواعد الاقتصادية، ويشكل خطرا كبيرا على مناخ الاستثمار محليا ودوليا ويضر بمصداقية الأسس الاقتصادية المتعارف عليها القائمة على نظرية تعظيم الربح والتي يمكن لصانعي السياسات الاقتصادية الاستناد إليها. ناهيك عما تؤدي إليه حركة الأموال المطلوب غسلها دون مراعاة الاعتبارات الاقتصادية من المنافسة غير المتكافئة مع المستثمر الجاد المحلي والأجنبي على السواء، باعتبار أن العملة الرديئة تطرد العملة الجيدة من التعامل،.راجع: أبو بكر الزهيري: مخاطر غسل الأموال على الاقتصاد الوطني، ورقة عمل مقدمة إلى ندوة غسل الأموال ومخاطرة، صنعاء-اليمن، 2008/11/18، ص3 وما بعدها، وراجع أيضا: سعيد عبد الخالق، القانون المصري رقم 80 لسنة 2002 الخاص بمكافحة غسل الأموال فلسفته وأهم ملامحه، موقع البوابة القانونية، ت.د 2008/6/13،على الرابط :
http://www.tashreaat.com/view_studies2.asp?std_id=26

حيث أصبحت التحركات المالية تدار بشكل تحركات رقمية وليس تداول مالي[1]، فأضحى من الضروري إيجاد تشريعات قانونية لمراقبة التحركات المالية للأموال المغسولة وعلى رأسها أموال تجار المخدرات والمسئولين الفاسدين..

وتتعدد مصادر الأموال المغسولة بداية بالمخدرات التي كانت تعد المصدر الأساسي لها، لأن أنشطة المخدرات هي التي أوجدت الوعاء الأكبر للأموال القذرة بفعل متحصلات عوائدها المرتفعة، إلا أن الواقع والدراسات أثبتت وجود العديد من الأنشطة الأخرى منها الفساد الإداري وخاصة في الدول النامية حيث نتج عنه ثروات باهظة غير مشروعة لأشخاص معدودين تحتاج لتكون محلا لغسيل الأموال كي يتمكن أصحابها من التنعم بها، وكذلك تجارة الأسلحة والرقيق والقمار.

وسيتم تناول جريمة غسيل الأموال وفقا للقواعد العامة في التشريع اليمني والجزائري، وجريمة غسيل الأموال عن طريق الإنترنت، وكذلك عن طريق بعض الوسائط لإيضاح مدى تناسب تلك القواعد للانطباق على الجريمة في حالة ارتكابها باستخدام التقنية الرقمية:

1- جريمة غسيل الأموال وفقا للقواعد التقليدية

تعرف جريمة غسيل الأموال وفقا لتعريف دليل اللجنة الأوروبية لغسيل الأموال الصادر لعام 1990بأنها (عملية تحويل الأموال المتحصلة من أنشطة جرميه بهدف إخفاء أو إنكار المصدر غير الشرعي والمحظور لهذه الأموال، أو مساعدة أي شخص ارتكب جرما ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم)، ويعتبر البعض بأن هذا التعريف يعد الأكثر شمولا وتحديدا لعناصر غسيل الأموال من بين التعريفات الأخرى التي تضمنتها عدد من الوثائق الدولية والتشريعات الوطنية [2].

---

(1) يقدر خبراء صندوق النقد الدولي حجم الأموال المغسولة سنويا مابين 620 مليار$ و 1.6 تريليون$، وأن مابين 50% إلى 70% يجري غسلها في الأسواق المالية في بنوك نيويورك ولندن ودول شرق أسيا، وأن مبلغ 300 مليون$ يتم غسلها من عائدات المخدرات، ويشير الخبراء بأن تلك المبالغ هي التي يتم غسلها عبر البنوك والمؤسسات المالية، أما الأموال المغسولة بشكل عام فتفوق ذلك بكثير. راجع : زياد على عربية، ((غسيل الأموال)) مجلة الأمن والقانون، صادرة عن أكاديمية الشرطة بدبي، ع1، يناير2004، ص79. ولمعرفة مزيد من إحصائيات الأموال المغسولة راجع: مجلة الفيصل، شهرية، صادرة عن مركز الملك فيصل للبحوث الدراسات الإسلامية، السعودية،ع371، مايو 2007، ص21،ص22.

(2) يونس عرب، جرائم غسيل الأموال، منشور على موقع منتدى كلية الحقوق - جامعة المنصورة، ت.د 2008/5/9.

http://www.f-law.net/law/showthread.php?t=8842

وجريمة غسيل الأموال كغيرها من الجرائم يشترط لقيامها أن تكون مجرمة بموجب نص قانوني عملا بمبدأ الشرعية الجنائية"لا جريمة ولا عقوبة إلا بنص"[1].

كما يجب أن يتوافر في الجريمة ركن مادي يتمثل بالأفعال التي تقوم بها الجريمة، وكذلك ركن معنوي يتحدد بالقصد الجنائي.

أ - الركن الشرعي لجريمة غسيل الأموال

لم يتناول القانون اليمني جريمة غسيل الأموال وكذلك القانون الجزائري إلا في الأعوام الأخيرة أسوة بغيرهما من التشريعات العربية، ومع أن القانون اليمني والجزائري قد صدرا في وقت متأخر إلا أنهما لم يتضمنًا نصوصا صريحةً تجرم ارتكاب جريمة غسيل الأموال باستخدام الإنترنت والتقنية الرقمية[2].

وبالعودة إلى النصوص القانونية في القانون اليمني والجزائري يتضح بأن الركن الشرعي للجريمة يتمثل بنصوص المادتين (1،3) من ق.ع.ي،والمواد (389مكرر، 389مكرر1، و389مكرر2) من ق.ع.ج وكذلك المواد(1،2) من القانون الجزائري الخاص بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.

حيث نصت المادة:(1) ع.ي على جريمة غسيل الأموال بأنها (كل عمل ينطوي على اكتساب أموال أو حيازتها أو التصرف فيها أو إيداعها أو استبدالها أو استثمارها أو تحويلها بقصد إخفاء المصدر الحقيقي لتلك الأموال المتحصلة عن الجرائم المنصوص عليها في المادة :(3) من هذا القانون) [3].

وتضمنت المادة(3) من ذات القانون على تجريم غسيل الأموال وإيضاح الأفعال التي يمكن أن ترتكب بها الجريمة حيث نصت على أن : (غسل الأموال جريمة يعاقب

([1]) وبذلك فقد قضي بأنه "يجب أن تتضمن الأحكام والقرارات عند الإدانة النصوص القانونية المطبقة وإلا وقعت تحت طائلة البطلان" (جنائي31 ديسمبر1989- ملف 36367) راجع: أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، ط1، الديوان الوطني للإشغال التربوية، 2000، ص303.

(2) تأخر المشرع اليمني في إصدار قانون بشأن مكافحة غسل الأموال حتى 2003، حيث اصدر القانون رقم (35) لسنة 2003بشأن مكافحة غسيل الأموال، ومع أنه يوجد مشروع قانون بشأن مكافحة غسل الأموال وتمويل الإرهاب إلا أنه لم يتضمن الإشارة بصورة صريحة إلى ارتكاب تلك الجرائم عن طريق الإنترنت، وكذلك الشأن في القانون الجزائري حيث لم يتضمن ق.ع رقم (04- 05) المؤرخ في 10 نوفمبر 2004، و القانون رقم (06- 23) المؤرخ في 20 ديسمبر2006 المعدل والمتمم لقانون العقوبات نصوصا قانونية تجرم غسل الأموال. وكذلك القانون رقم (05 -01)المؤرخ في6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما .

(3) المادة(1) من القانون اليمني رقم(35)لسنة 2003بشأن مكافحة غسيل الأموال.

عليها بموجب أحكام هذا القانون ....) [1] ، وأشارت المادة إلى عدد من الأفعال سوف يتم الإشارة إليها أثناء تناول الركن المادي للجريمة.

ونصت المادة: (389 مكرر) من ق.ع.ج على الأفعال التي ترتكب بها جريمة غسيل الأموال وكذلك المادة (2) من قانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما[2]

كما تضمنت المادة (389 مكرر1) على عقوبة جريمة غسيل الأموال، أما المادة (389 مكرر2) فقد نصت على جريمة تبييض الأموال إذا ارتكبت على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني، وكذلك إذا تم ارتكابها في إطار جماعة إجرامية بقولها (يعاقب كل من يرتكب جريمة تبييض الأموال على سبيل الاعتياد، أو باستعمال التسهيلات التي يمنحها نشاط مهني، أو في إطار جماعة إجرامية بالحبس من عشر(10) سنوات إلى عشرين(20)سنة وبغرامة من 4.000.000 د.ج إلى 8.000.000دج)[3].

من خلال النصوص السابقة يتضح بأن المشرع اليمني قد عرف جريمة غسيل الأموال، بخلاف المشرع الجزائري، حيث لم يضع تعريفا جامعا لغسيل الأموال، واكتفى بذكر الحالات التي يمكن أن تتم بها الجريمة[4].

كما حددت تلك النصوص في كلا القانونين الجرائم التي يمكن أن تكون الأموال الناتجة عنها محلا للغسل، إذا تحققت أفعال التمويه، أو الاكتساب، أو التصرف فيها، أو غير ذلك من الأفعال التي تخفي مصدرها والتي سيتم الإشارة إليها أثناء تناول الركن المادي للجريمة.

فجريمة غسيل الأموال هي جريمة لاحقة لاقتراف جريمة، الهدف منها إخفاء العوائد التي تم تحقيقها نتيجة لاقتراف جرائم أخرى، حيث لا يكون أمام المجرمين إلا

(1) راجع المادة(3) من القانون اليمني رقم(35) لسنة 2003 بشأن مكافحة غسيل الأموال.
(2) المادة (389)مكرر من القانون رقم (04- 05) المؤرخ في 10 نوفمبر 2004المُعدِل والمُتمِم للأمر رقم (66-156)المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات، والمادة(2)من القانون رقم (50 - 01)المؤرخ في 6فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.
(3) راجع المادة (389مكرر 1)، والمادة (389مكرر2) من ق.ع.ج رقم (06- 23 المؤرخ في 20 ديسمبر 2006.
(4) راجع المواد (389مكرر، و389 مكرر1، و389 مكرر2) من ق.ع.ج، وراجع أيضا: المادة (2) من القانون رقم (05-1)المؤرخ في 6فبراير سنة 2005 بشأن الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما حيث لم تتضمن أي من هذه المواد تعريفا لجريمة غسيل الأموال واكتفت بذكر الأفعال التي ترتكب بواسطتها.

إخفاء تلك الأموال القذرة تحت غطاء شرعي ليتاح لهم استعمالها[1]، وبالتالي وحتى يتم لعصابات الإجرام التخلص من تلك الأموال القذرة والخروج من المأزق الذي قد يقعوا فيه بسبب الأموال غير المشروعة التي يحصلون عليها، وقد تكون سببا في كشفهم والحد من أنشطتهم، فإنهم يعملون على غسلها وتدويرها حتى يصعب متابعتها ومعرفة مصدرها الحقيقي.كما يلاحظ بأن النص الوارد في المادة(2) من القانون الجزائري الخاص بالوقاية من تبييض الأموال وتمويل الإرهاب قد ورد بنفس الألفاظ التي وردت في المادة: (389مكرر) من قانون العقوبات باستثناء لفظ "تأتت"في ق.ع استبدل في قانون تبييض الأموال بلفظ تحصلت، وكذلك لفظ "والتحريض" استبدل بلفظ أو التحريض وبالتالي فإن نص المادة (2) من قانون الوقاية من تبييض الأموال قد نقل حرفيا من قانون العقوبات.

ب - الركن المادي لجريمة غسيل الأموال

يتحقق الركن المادي لجريمة غسيل الأموال بتحقق عدد من الأفعال بشرط أن تستهدف تلك الأفعال الأموال الناتجة عن إحدى الجرائم بشكل عام، وفي القانون اليمني تم الاقتصار على الأموال الناتجة عن الجرائم المحددة بنص المادة (3) ع.ي، وتشمل عدد من الجرائم المالية[2].

وتتمثل الأفعال التي تمثل الركن المادي في جريمة غسل الأموال بالتالي:

- اكتساب، أو حيازة، أو التصرف، أو إيداع، أو استبدال، أو استثمار، أو تحويل الأموال الناتجة عن الجرائم بقصد إخفاء المصدر الحقيقي لها.

([1]) راجع: احمد حسن، جرائم غسيل الأموال في التشريع العراقي، بحث منشور على الشبكة المعلوماتية متاح في تاريخ 10/ 2009/9 على الرابط:
http://www.iraqja.org/judicalsheet3/research/gasil_amwal_raaed.htm

(2) والجرائم التي حددتها المادة (3)ع.ي وجعلت جرائم غسيل الأموال تقتصر على الأموال الناتجة عنها هي:
- الجرائم المنصوص عليها في قانون مكافحة جرائم الاختطاف والتقطع.
- السرقة أو اختلاس الأموال العامة أو الاستيلاء عليها بوسائل احتيالية أو الرشوة وخيانة الأمانة.
- تزوير وتزييف الأختام الرسمية والعملات والأسناد العامة.
- الاستيلاء على أموال خاصة معاقب عليها في قانون الجرائم والعقوبات.
- التهريب الجمركي.
- الاستيراد والاتجار غير المشروع للأسلحة.
- زراعة المخدرات أو تصنيعها أو الإتجار بها وكذا صناعة الخمور أو الإتجار بها وغيرها من الأنشطة المحرمة شرعا.

وقد تم إضافة عدد من الجرائم في مشروع قانون مكافحة غسيل الأموال وتمويل الإرهاب.

- إخفاء المصدر الحقيقي للأموال غير المشروعة، أو إعطاء تبرير كاذب عن هذا المصدر.
- تحويل الأموال، أو استبدالها في القانون اليمني، وأضاف القانون الجزائري فعل النقل بجانب التحويل، والتحويل يكون من عملة إلى أخرى، أو من أموال إلى شي آخر، مجوهرات مثلا، أما النقل فيكون بكافة الأفعال التي يمكن من خلالها أن يتم نقل الأموال سواء باستخدام الوسائل التقليدية، أم الوسائل الحديثة عبر البنوك أو المؤسسات المصرفية، وما إلى ذلك من وسائل التقنية الحديثة[1]، ويكون التحويل أو النقل مع العلم بأنها غير مشروعة لغرض إخفاء أو تمويه مصدرها أو مساعدة شخص على الإفلات من العقاب أو المسئولية.
- فعل الاشتراك، أو المساعدة، أو التواطؤ، أو التأمر على ارتكاب الجريمة، أو التحريض وتسهيله، أو إسداء المشاورة بشأنها
- تملك الأموال غير المشروعة، أو حيازتها، أو استخدامها، أو توظيفها لشراء أموال منقولة أو غير منقولة[2].

والأفعال التي يتكون منها الركن المادي في جريمة غسل الأموال تفترض وقوع جريمة سابقة عليها، هي الجريمة التي تحصل منها المال المراد غسله، وهي بمثابة ركن مفترض في جريمة غسل الأموال وتتمثل في ارتكاب جريمة أولية يعقبها جريمة تابعة [3]، فإذا تحققت تلك الأفعال واستهدفت الأموال الناتجة عن إحدى الجرائم، فقد تحققت جريمة غسيل الأموال. وتقوم الجريمة بغض النظر عما إذا كان الجاني قد قام باقتراف الفعل بنفسه، أو أن فعله اقتصر على الاشتراك، أو المساعدة، أو التحريض، أو التستر على ارتكاب أي من الجرائم السابق ذكرها.

---

(1) ومن ذلك قيام مجموعة من قراصنة المعلوماتية بتبييض أموال عبر استخدام النقود الإلكترونية وتدويرها عبر عشرات البنوك في أوربا الشرقية، وذلك بعد قيامهم باختراق بطائق الائتمان لعدد من الشركات في الولايات المتحدة، والحصول على أموال كثيرة. تفاصيل القضية على موقع وزارة العدل الأمريكية، ت.د 2008/8/8 على الرابط:
http://www.usdoj.gov/criminal/cybercrime/index.html

(2) راجع المادة(3) من القانون اليمني رقم(35)لسنة 2003بشأن مكافحة غسيل الأموال. والمادة (389 مكرر) من ق.ع.ج وكذلك المادة (2) من القانون الجزائري بشأن الوقاية من تبييض الأموال وتمويل الإرهاب.

(3) راجع مراد رشدي،غسل الأموال عبر الوسائل الإلكترونية، بحث قدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، الإمارات العربية المتحدة، من 26 /2003/4 إلى 2003/4/28، منشور على موقع منتدى هيئة التحقيق والادعاء بالمملكة العربية السعودية، ت.د 2006/1/8على الرابط:

http://vb.bip.gov.sa/archive/index.php?t-6909.html

وقد أورد المشرع اليمني فعل التحويل ولم يورد في نصوصه فعل نقل الأموال كما فعل المشرع الجزائري في نص المادة (2)التي شملت فعلي التحويل والنقل للأموال[1].

وفعل النقل يختلف عن فعل التحويل، في كون النقل يتم عبر حركة مادية يتم بواسطته نقل المال من مكان إلى مكان أخر، وقد يكون النقل داخليا في إطار الحدود الإقليمية للبلد الواحد، كما قد يكون وهو الغالب الأعم عبر الحدود إلى دول أخرى، أما تحويل الأموال فإنه يتمثل في إجراء عمليات مصرفية أو غير مصرفية سواء عن طريق مؤسسات مالية رسمية كالبنوك، أم غير رسمية يكون الغرض منها في كل الأحوال تحويل المال إلى شكل آخرسواء من عُمْلَة محلية إلى عُمْلَة عالمية أمن عُمْلَة إلى منقول ثمين، وغير ذلك من الأشكال التي تؤدي إلى قطع الصلة الظاهرة بين المال ومصدره حتى يبدو كما لو كان مالا ناتجا عن مصدر آخر غير الجريمة[2].

ومع أن البعض يخرج الأفعال المتعلقة بالفساد من جرائم غسيل الأموال حتى لو اتخذت تلك الأفعال مظاهر توحي بأن تلك الأموال مشروعة بهدف التمويه[3]، إلا أن ذلك يبدو غير صحيح ويتنافى مع المعايير التي وضعت بشأن غسيل الأموال، لكون الفساد الإداري وما ينتج عنه من فساد مالي يجعل أصحاب تلك الأموال يعملون جاهدين على إخفاء مصادرها وظهورها بالمظهر الشرعي، فغالبا ما يعمد هؤلاء إلى شراء عقارات، أو الدخول في مساهمات عبر شركات، وقد تكتب تلك العقارات والأسهم بأسماء آخرين سواء أكانوا من أقاربهم أم أصدقاؤهم، كما يتم تهريب تلك الأموال إلى الخارج ومن ثم استثمارها وغيرها من الأفعال التي تموه عن المصدر الحقيقي لها بحيث تبدو وكأنها أموال مشروعة.

---

(1) تضمنت فعل النقل بجانب فعل التحويل في جريمة غسل الأموال المادة (389 مكرر) من ق.ع.ج والمادة (2) من قانون الوقاية من تبييض الأموال وتمويل الإرهاب.

(2) مراد رشدي، غسل الأموال عبر الوسائل الإلكترونية، مرجع سابق، ص20 .

(3)أحمد غالب رئيس لجنة مكافحة غسيل الأموال باليمن، تعقيب على تقرير اللجنة الأمريكية بشأن دور اليمن في مكافحة غسيل الأموال، ورد في صحيفة المؤتمر نت الصادرة يوم السبت-2007/7/14، وجريدة الثورة، 2007/7/14.

كل تلك الأفعال لا تدع مجالا للشك أنها تدخل في نطاق غسيل الأموال خاصة في البلدان التي لا توجد فيها رقابة على مصادر الأموال[1].

وإذا كان القانون اليمني قد حدد الجرائم التي ترتبط بغسيل الأموال، وركز على الجرائم المالية أو التي يمكن أن ينتج عنها سلب مال الغير أو اختلاسه، فإن أغلب الفقهاء قد اعتبروا أن كافة الجرائم يمكن أن تكون مرتبطة بغسيل الأموال طالما نتج عن اقترافها الحصول على أموال يمكن أن تكون عرضة للغسل إذا ما ارتبطت بأحد الأفعال المذكورة في نصوص القانون، لكون القانون الذي يحدد جرائم معينة ويجعلها دون غيرها من الجرائم هي التي لها ارتباط بغسيل الأموال، يعد تخصيصا بعد تعميم ولا يصلح لبراءة الأموال الناجمة عن جرائم غير التي اعتبرها القانون جرائم غسيل الأموال، بالإضافة إلى أنه يخالف التشريع العقابي العالمي المقارن، الذي يقرر قاعدة عامة في شأن الأموال الناتجة عن جريمة والتي مفادها" أن كل الأموال المتحصلة من

(1) ومثال لقضية الفساد من قبل بعض المسئولين قضية لوزارينكو (رئيس الوزراء الأوكراني السابق) حيث تمت إدانته والحكم عليه من قبل القضاء السويسري بتاريخ 2000/6/29، لقيامه بأنشطة غسيل أموال تبلغ 880 مليون دولار في الفترة ما بين 94 - 97 ، من بينها 170 مليون تم غسيلها عبر حسابات سويسرية، و اعترف بعملية غسل 9 ملايين فقط، وقد كانت العقوبة هي الحبس لمدة 18 شهرا، بعد أن تم اعتقاله من قبل السلطات السويسرية في كانون الثاني عام 1998 عندما دخل سويسرا بجواز سفر بنمي (بنما) مزور وأطلق صراحة بالكفالة البالغة 3 مليون دولار أمريكي، وما لبث أن غادر إلى الولايات المتحدة في عملية لجوء سياسي، وتم إلقاء القبض عليه واحتجازه ومن ثم محاكمته مع شخص أخر هو بيتر كيرتشينكو، الذي يعتقد بأنه هو الذي قام بتنفيذ عمليات غسيل الأموال، وتتضمن اللائحة اتهامهما بتحويل 114 مليون دولار أمريكي إلى البنك التجاري في سان فرانسيسكو، والباسفيك بنك، ووست أميركا بنك، وبنك أوف أميركا، وميرل لينش، ومؤسسة افليت بوستن روبيرتسون خلال الأعوام من 94 -99، إضافة إلى توجيه الإتهام لهما بشراء موجودات ومشاريع في أمريكا خلال عامي 97 - 98 نقدا، والاحتيال وتحويل أموال مسروقة إلى الولايات المتحدة، وقد كشفت هذه القضية جراء أنشطة تحقيق امتدت إلى عامين كاملين، تعاونت فيها الشرطة الفدرالية الأمريكية وأجهزة التحقيق في سويسرا إضافة إلى جهات أمنية في روسيا الاتحادية وأوكرانيا، وجرى التحقيق في مصادر هذه الأموال التي تبين أنها نجمت عن استغلال رئيس الوزراء لمهام وظيفته، وجراء تلقيه مبالغ نقدية من أفراد ومؤسسات ورشاوى لتسهيل تنفيذهم لأعمالهم، وتعد هذه القضية أول قضية وفق قانون غسيل الأموال الأمريكي تستخدم الإجراءات فيها بشأن أنشطة ارتكبت خارج الولايات المتحدة وتتعلق بشخص من خارجها، وتستند المحكمة في اختصاصها إلى أن جزءا من أنشطة الجريمة في بعض الحالات قد ارتكب داخل الولايات المتحدة، وجزءا آخر من الأنشطة كانت الولايات المتحدة فيه محطة لعمليات التحويل وإدماج المبالغ محل الجريمة ضمن النظام المالي الأمريكي وإعادة تحويلها إلى جهات أجنبية أخرى، إلى جانب إيداع النقود في بنوك الولايات المتحدة وشراء موجودات ومشروعات فيها. راجع: يونس عرب، ماهية ومخاطر غسيل الأموال، مقال منشور على موقع حواس للمحاماة، وكذلك موقع مدونة مدينتي، ت.د 2/ 2008/5 على الرابطين:

http://hawassdroit.ibda3.org/montada-f17/topic-t420.htm

http://samirlawer.elaphblog.com/posts.aspx?U=995&A=6195

جريمة تصلح لان تكون محلا لغسيل الأموال وإنتاج عوائدها"[1]، وذلك مقر في عدد من التشريعات[2].

ونحن نؤيد الرأي السابق الذي لا يجعل نطاق جريمة غسيل الأموال ترتبط بجرائم معينة، إذ المعيار" أن كل جريمة ينتج عنها عوائد مالية تكون عرضة لغسلها تدخل في عداد الجرائم المرتبطة بغسل الأموال إذا ما تلتها أفعال تخفي مصدرها الحقيقي- الغير مشروع- وتظهرها بمظهر الأموال المشروعة"، وعلى سبيل المثال من يقتل فلان من الناس بهدف الاستيلاء على أمواله فإنه يكون قد حصل على تلك الأموال بطريقة غير مشروعة، وبالتالي فقد يفكر في غسلها، ليس بهدف عدم اكتشافه في جريمة القتل فحسب، بل لعدم اكتشاف مصدر الأموال التي حصل عليها دون حق، وعلى وجه الخصوص في البلدان ذات الأنظمة المالية الدقيقة وهكذا بقية الجرائم.

وخلاصة ما سبق فإن الأفعال التي يقوم بها الركن المادي في جريمة غسيل الأموال تدخل في إطار التوظيف والتمويه والتكامل أو الدمج[3].

ويقصد بالتوظيف " توظيف الأموال غير المشروعة في صورة إيداعات في المؤسسات والبنوك وشراء أسهم، أو مؤسسات مالية، أو تجارية، أو غيرها من الأنشطة التي تمارس لتوظيف تلك الأموال غير المشروعة.

ويقصد بالتمويه: خلق مجموعة معقدة من العمليات التي تهدف إلى التمويه عن مصدر تلك الأموال.

ويقصد بالتكامل أو الدمج: ضخ تلك الأموال في الاقتصاد مرة أخرى، حيث تصبح كأنها أموال مشروعة معروفة المصدر ويصعب التحري عنها.

وكمثال على صعوبة التحري عن مصادر تلك الأموال : ما يتم التعامل به بواسطة بطاقة الائتمان، فمن يقوم بالتعامل عبر هذه البطاقة من دولة ما ويتمكن من الحصول على سلع وما إلى ذلك من خدمات تقدم عن طريق تلك البطاقة، وقد تكون الجهة مقدمة السلع أو الخدمة في دولة أخرى، واستقطاع المبلغ يكون عبر الجهة المصدرة لتلك

---

(1)عمر محمدي أبو بكر يونس، يوسف أمين شاكير،غسل الأموال عبر الإنترنت وموقف السياسة الجنائية، ط1، دار النهضة العربية، القاهرة، 2004، ص10.

(2) ومن التشريعات التي جرمت غسيل الأموال الناتجة عن أي جرائم كانت ولم تجعلها قاصرة على جرائم معينة هو التشريع الفرنسي، واتفاقية المجلس الأوربي الموقعة في ستراسبورج في 2005/11/18، راجع عبد الفتاح سليمان، مرجع سابق، ص44.

(3) عمر عيسى ألفقي، الجرائم المعلوماتية، دار الكتب الجامعي الحديث، الإسكندرية، 2006، ص148.

البطاقة، والتي قد تكون في دولة ثالثة، ويستطيع بيع تلك البضاعة والحصول على قيمتها مرة أخرى، وقد يتم إيداع المبلغ في بنك الدولة التي تم السحب أو التعامل فيها، وبذلك تكون قد أضحت معروفة المصدر، ويتم التعامل مع تلك الأموال على أنها شرعية[1].

ج - الركن المعنوي في جريمة غسيل الأموال

جريمة غسل الأموال جريمة عمدية لا يتصور أن ترتكب بطريق الخطأ أو الإهمال، وبذلك فإن الركن المعنوي في جريمة غسيل الأموال يقوم على القصد الجنائي العام بعنصرية العلم والإرادة، علم الجاني بالعناصر المكونة للجريمة وإقدامه على ارتكاب تلك الأفعال بإرادته واختياره.

فيجب أن يعلم الجاني انه يقوم بأفعال وعمليات معقدة من شأنها في نهاية الأمر أن تظهر تلك الأموال غير المشروعة بصفة المشروعية، أو أن يعلم بأنه يقوم بنفسه، أو بالاشتراك أو المساعدة مع مالكي تلك الأموال الغير مشروعة، بأفعال من شأنها إخفاء المصدر الحقيقي لتلك الأموال والتستر عليها.

ويجب أن يعلم بأنه يقوم بتحويل، أو نقل أموال أو ممتلكات ناتجة عن عوائد إجرامية، وأن يكون ذلك بغرض التمويه عن المصدر غير المشروع لتلك الأموال.

كما يتطلب لقيام الجريمة أن يعلم الفاعل بأن الأموال التي يقوم بتملكها، أو نقل حيازتها، أو استخدامها، أو إخفائها، أو تمويه طبيعتها أو مصدرها أو مكانها أو حركتها من عائدات مصادر غير مشروعة مما نص عليها القانون.

وبجانب علمه بكل ما ذكر فيجب أن تتجه إرادته إلى اقتراف تلك الأفعال غير مبالٍ بما سيترتب عليها من نتائج.

د - عقوبات جريمة غسيل الأموال

يعاقب كل من ارتكب جريمة غسل الأموال طبقا لنص المادة: (3) من قانون غسيل الأموال اليمني بالسجن مدة لا تزيد عن خمس سنوات، مع عدم الإخلال بأي عقوبة أشد بموجب قانون آخر[2] .

كما تكون العقوبة السجن مدة لا تزيد على ثلاث سنوات أو بغرامة لا تزيد على (500,000) خمسمائة ألف ريال لكل من خالف أحكام المادة :(5)من ذات القانون،

---

(1) عمر عيسى ألفقي، مرجع سابق، ص165.
(2) المادة(21) من قانون غسيل الأموال اليمني رقم(35)لسنة 2003.

حيث تطبق العقوبة الأخيرة على المؤسسات المالية في حالة عدم إبلاغ وحدة مكافحة غسيل الأموال بأي عملية تستهدف غسل الأموال إذا تحقق لديها ما يؤكد ذلك، وتطبق ذات العقوبة على المؤسسات في حال إشعار المتعاملين لديها بأنهم متابعون من الجهات المعنية، وبأنها ستقوم بالإبلاغ عنهم، أو تسريب، أو إفشاء أي معلومات ، أو عن أنشطتهم، أو الامتناع عن تقديم البيانات والوثائق لوحدة مكافحة غسل الأموال، أو للجهات القضائية، أو اعتراض تنفيذ أي قرار صادر من الجهات القضائية يتعلق بأي جريمة من جرائم غسل الأموال .

كما تضمن القانون عقوبات تكميلية هي عقوبة مصادرة كافة الأموال والعوائد التي تم الحصول عليها من الجرائم المتعلقة والمرتبطة بغسل الأموال، إضافة إلى إلغاء الترخيص بالنسبة لمؤسسات الصرافة أو غيرها من الجهات التي تساهم في أنشطة لها علاقة بغسيل الأموال، ووقف النشاط أو أي عقوبة تكميلية أخرى منصوص عليها في القوانين النافذة .

كذلك فقد نص ق.ع.ج وقانون الوقاية من عملية غسيل الأموال وتمويل الإرهاب على نوعين من العقوبات، عقوبات أصلية وعقوبات تكميلية[1].

وتمثل العقوبات الأصلية بالعقوبات التالية:

- الحبس من خمس (5)إلى عشر(10)سنوات وبغرامة من 1.000.000دج إلى 3.000.000دج لكل من يقوم بعملية تبييض الأموال [2] .
- الحبس من عشر(10) سنوات إلى عشرين(20)سنة وبغرامة من 4.000.000دج إلى 8.000.000دج لكل من يرتكب الجريمة على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني، وكذلك إذا تم ارتكابها في إطار جماعة إجرامية[3].

---

(1) واليمن كغيرها من الدول العربية قلما تجد محاكمة لجرائم غسيل أموال، ومن ثم تطبيق العقوبات التي ينص عليها القانون، باستثناء بعض القضايا منها قضية واحدة في جمهورية مصر العربية تم مقاضاة متهم وزوجته تخصصا في سرقة رواد البنوك ومكاتب الصرافة وحققا ثروة مليوني جنيه وقاما بشراء شقق فاخرة وسيارات، تم حصرها لبيعها وتطبيق قانون غسيل الأموال عليها، وإعادة مستحقات الضحايا. انظر.جريدة الأخبار الإلكترونية، ع 17356، الأربعاء 5 ديسمبر 2007 م، على الربط:
http://www.elakhbar.org.eg/issues/17356/1100.html

(2)راجع: المادة (389 مكرر1)من القانون رقم (06- 23)المؤرخ في 20 ديسمبر 2006المَعدِل والمَتمِم للأمر رقم(66- 156) المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات (ج.ر 84 ص26).

(3) المادة (389 مكرر2) من القانون نفسه.

- وتكون عقوبة المحاولة في ارتكاب جرائم تبييض الأموال المنصوص عليها، هي العقوبة المقررة للجريمة التامة[1].

وبجانب العقوبات الخاصة بتبييض الأموال وبهدف الوقاية من الجريمة فقد نص القانون على عدد من العقوبات التي تهدف إلى الحد والوقاية من الجريمة وهي:

- معاقبة كل من يقوم بدفع أو يقبل دفعا يفوق مبلغا يتم تحديده عن طريق التنظيم خرقا لأحكام المادة(6) من قانون الوقاية من تبييض الأموال، بحيث لا يلتزم بالدفع عن طريق القنوات البنكية والمالية بغرامة من 50.000 دج إلى 500.000 دج.
- وتكون العقوبة الغرامة من 100.000 دج إلى 1000.000 دج لكل خاضع يمتنع عمدا وبسابق معرفة، عن تحرير أو إرسال الإخطار بالشبهة المنصوص عليها في القانون دون الإخلال بأي عقوبة أشد أو بأي عقوبة تأديبية أخرى.
- بينما تكون العقوبة لمسيّرين وأعوان الهيئات المالية الخاضعين للإخطار بالشبهة هي الغرامة من 200.000 دج إلى 2.000.000 دج دون الإخلال بأي عقوبة أشد أو عقوبة تأديبية أخرى، وذلك في حالة إبلاغهم عمدا لأصحاب الأموال أو العمليات موضع الإخطار بالشبهة بوجود هذا الإخطار، أو إطلاعه أو إطلاعهم على المعلومات حول النتائج التي تخصه أو تخصهم[2].

أما العقوبات التكميلية وفقا للقانون الجزائري فتتمثل بالتالي [3]:-

- مصادرة الأملاك التي موضوعها جرائم غسيل الأموال بما فيها العوائد والفوائد الأخرى الناتجة عن ذلك، وتكون المصادرة بمقدار العائدات فقط في حالة اندماج تلك العائدات مع أموال مشروعة.
- مصادرة الوسائل والمعدات المستعملة في ارتكاب الجريمة، بموجب حكم يتضمن تعيينها وتحديد مكانها.
- جواز الحكم بالمنع من الإقامة على الإقليم الوطني بصفة نهائية أو لمدة عشر سنوات على كل أجنبي مدان .

---

(1) راجع: المادة (389 مكرر 3) من القانون رقم (04- 15) المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات.

(2)المواد (33،31،32) من القانون رقم (05-1)المؤرخ في 6 فبراير سنة 2005 بشأن الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم.

(3) راجع : المواد (من 389 مكرر4 إلى 389 مكرر6) من القانون رقم (04- 15) المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات.

ويعاقب الشخص المعنوي بالعقوبات التالية[1]:

- بعقوبة لا تقل عن أربع مرات الحد الأقصى للغرامة المقررة على الشخص الطبيعي.
- مصادرة الممتلكات والعائدات التي تم تبيضها.
- مصادرة الوسائل والمعدات التي استعملت في ارتكاب الجريمة.
- كما يمكن للجهة القضائية أن تقضي بالإضافة إلى ذلك بالمنع من مزاولة نشاط مهني أو اجتماعي لمدة لا تتجاوز خمس سنوات، وحل الشخص المعنوي.

2- جريمة غسيل الأموال بواسطة الإنترنت

بعد أن أصبحت أغلب التعاملات تتم عبر الإنترنت، فقد أضحت وسيلة ميسرة لارتكاب جريمة غسيل الأموال، نظرا لاعتبارها وسيلة سهلة للتواصل والتخطيط بين أطراف الجريمة لاقتراف الجرائم المنظمة بما فيها جريمة غسيل الأموال.

ولكون القانون اليمني والقانون الجزائري لم يتضمنا النص بصورة صريحة على جريمة غسيل الأموال عبر الإنترنت، فهل تلك النصوص التقليدية تفي بالغرض المطلوب لمواجهة تلك الجريمة المقترفة عبر العالم الافتراضي؟

فمع تحول الإنترنت إلى وسيلة يتم عبرها إجراء المزيد من العمليات التجارية الدولية، فإن الأفعال التي يمكن أن ترتكب من خلالها جريمة غسل الأموال بلا شك ستتم بإتباع أسلوب تقني عن طريق إصدار الفواتير الزائدة أو الناقصة عن الأسعار الحقيقية.

كما توفر مزادات السلع التي تتم بواسطة الإنترنت فرص مماثلة لنقل الأموال من خلال عملياتشراء قانونية ظاهرياً ، ولكن بدفع ثمن يفوق بكثير الثمن الحقيقي لتلك السلع.

وكذلك فقد يتم تهريب الأموال المراد غسلها عن طريق الرسائل الإلكترونية، والتي يتم من خلالها توجيه رسالة إلكترونية من المجرم أو قريبة إلى شخص أخر في دولة أخرى، يعرض عليه استثمار أمواله التي لا يستطيع أن يستثمرها هو، أو مساعدته في تحويل أمواله إلى الدولة التي يقيم فيها متلقي الرسالة بسبب مشاكل تجعله لا يستطيع

(1) راجع المادة (389 مكر 7) من القانون رقم (04- 15) المؤرخ في 10 نوفمبر 2004.

أن يستثمر أمواله في الدولة التي ينتمي إليها مقابل نسبة معينة يتم الاتفاق عليها تتبعها إجراءات التحويلات المالية[1].

بالإضافة إلى ذلك فإن انتشار تحويل الأموال والقيام بالأعمال المصرفية إلكترونيا يزيد من فرص إخفاء تحركات نتائج الجرائم باستعمال مجموعة متزايدة من المعاملات المالية غير القانونية والأمثلة على ذلك كثيرة [2].

ففي ظل العالم الرقمي فإن المجرمين في مجال المعلوماتية قد اتجهوا إلى استخدام الوسائط الإلكترونية لارتكاب جريمة غسيل الأموال، حيث يمكن باستخدام هذه الوسائط تحريك المال عن بعد في مختلف مراحل وعمليات الغسل، سواء في مرحلة فتح الحساب في أحد المصارف عن طريق الحاسب الآلي مستعينا بشبكة الإنترنت مع اختيار اسم مستعار أو شفرة أو رموز معينة، ثم تحريك المال من مكان إلى مكان حتى لا تتمكن أي جهة كانت من تتبعه ثم القيام بعد ذلك بتكديس المال في مشروعات وهمية بأن يتم الإعلان عنها على شبكة الإنترنت، ويتم فتح باب المساهمة العامة عن طريق أسهم

---

(1) وإيضاحا لقيام بعض المجرمين بمحاولة غسيل الأموال عن طريق الإنترنت نورد قضيتين :
الأولى :تتمثل في تلقي أحد المصريين يعمل في بنك مصري رسالة الكترونية من إحدى السيدات تدعى كرستين اندمير ملخصها أن لها ثروة كبيرة انتقلت إليها من زوجها المتوفى، وبسبب أن الدولة قد حجزت على بعض أموال زوجها وأصدرت في حقها قرار بالإقامة الجبرية بحيث لا تستطيع أن تحول أي أموال من بلدها كندا وأن لهم مبلغ 4 مليون دولار في أحد البنوك السويسرية تريد أن يساعدها في تحويلها إلى مصر، فإذا أبدى موافقته فعلية التواصل مع محامي العائلة وإرسال رقم حسابه بشرط أن يتم استثمار 20%من المبلغ في مصر ويرسل الباقي بحسب ما يتم الاتفاق بينهم، وحددت نسبة له مقابل ذلك، وبعد قيام الشاب المصري بالإبلاغ عن القضية و متابعتها من قبل مباحث جرائم الحاسب الآلي، اتضح أن كرستين هي زوجة رجل من كبار تجار المخدرات وهي تريد غسل أموال زوجها بعيدا عن الرقابة .
والثانية :تتمثل في قيام فتاة بالتراسل مع شاب مصري أوضحت له بأنها تلقت ثروة كبيرة هي ووالدتها من والدها المتوفى ولأسباب سياسية فقد تم مصادرة معظم أموال والدها، وتخاف من مصادرة ما تبقى، وإذا ما تم ذلك فستكون هي ووالدتها في طريقهما إلى الفقر، وتريد منه أن يساعدها في نقل 100مليون$ إلى مصر مقابل حصوله على نسبة 5%، وإذا أراد أن يتأكد فعليه الاتصال بمحامي العائلة، وإذا أبدى موافقته فسيتم مساعدته والاتفاق معه في كيفية تحويل تلك الأموال، وعقب ذلك قام الشاب المصري بإبلاغ مباحث جرائم الحاسوب، وهي بدورها تابعت القضية وأتضح، بأن الفتاة هي ابنة أكبر تاجر سلاح في كولومبيا وأنها تريد غسل أموال أبيها الغير شرعية. راجع: مجلة أخبار الحوادث المصرية،ع.17،672 فبراير2005 الموافق 8 محرم 1426.

(2). ولعل أبرز مثال على ذلك - رغم عدم نجاحه - ما حصل في شهر أكتوبر عام 2000م مع بنك صقلية. فقد ابتكرت مجموعة من حوالي 20 شخصاً، بعضهم يرتبط بعائلات المافيا، بمساعدة شخص من داخل البنك، الحصول على نسخة رقمية طبق الأصل لنظام وصل البنك بشبكة الإنترنت، وبعد ذلك قررت المجموعة استعمال هذه النسخة الرقمية المطابقة للأصل لتحويل مسار حوالي 400 مليون دولار كان الاتحاد الأوروبي قد خصصها لتمويل مشاريع إقليمية في صقلية، وكان من المقرر غسل تلك الأموال عبر مؤسسات مالية مختلفة منها بنك الفاتيكان وبنوك في سويسرا والبرتغال، إلا أن الخطة أحبطت عندما باح بالسر شخص من المجموعة إلى السلطات الرسمية، ومع ذلك فقد كشفت هذه المحاولة الفاشلة بصورة واضحة للغاية بأن الجريمة المنظمة تجد فرصاً لها لتحقيق أرباح نابعة من نمو العمل المصرفي الإلكتروني والتجارة الإلكترونية، راجع: فيل وليامز، الجريمة المنظمة وجرائم الشبكات الإلكترونية، دراسة متاحة على موقع منتدى هيئة الادعاء العام بالمملكة العربية السعودية، ت. د 2009/3/8، على الرابط:

http://vb.bip.gov.sa/showthread.php?t=5202

محددة القيمة تدخل إلى حساب المشروع إلكترونيا عن طريق فتح صفحة خاصة (Side) لتلقي هذه الأموال التي تدخل إليه مختلطة بأمواله غير المشروعة فتغسلها جزئيا، ثم يعلن بعد مرور وقت معين عن تصفية هذا المشروع زاعما تعرضه لخسائر، ويتم بعد ذلك توزيع الحصص على أصحابها مع هامش الفائدة المتفق عليها، ويقوم بسحب أمواله القذرة في هذه المرحلة باعتبارها ناتجة عن مشروع، ويبدأ في المرحلة الثالثة والأخيرة في استثمار هذا المال في مشروعات حقيقية تدخل في دائرة الاقتصاد القومي[1].

3- الوسائط التي يمكن استخدامها في غسيل الأموال

أ- **البنوك:** غسيل الأموال عن طريق البنوك هو الطريقة الأكثر شيوعا سواء بالطرق التقليدية أم الإلكترونية وتتم عبر مراحل هي:

- **الإيداع**

ويتم عن طريق إيداع المبالغ المالية في البنك عن طريق الحساب الذي يتم فتحه باستخدام الطرق العادية، أو باستخدام الإنترنت، ومرحلة الإيداع الإليكتروني قد لا تتناسب مع غسل الأموال، ذلك أن هذا النوع من الإيداع يتم بمبالغ ضئيلة لا تتناسب مع حجم المال المغسول، لذلك فإنه في الغالب الأعم يتم الإيداع بالطريق المختلط التقليدي والإلكتروني معا.

- **الاستثمار في العقارات والمنقولات**

بمجرد إيداع الأموال في البنك، وبموجب طبيعة عمل البنك فإنه يقوم باستثمارها ضمن غيرها من الأموال المودعة لديه، وبذلك فإن البنوك تساهم بطريقة أو بأخرى في غسل تلك الأموال بخلطها ضمن أموال المودعين، واستثمارها دون معرفة حقيقة مصدرها.

كما أن المجرمين قد يقومون بأنفسهم باستثمار تلك الأموال بعد إيداعها، وذلك بطلب قروض تحت ستار الودائع التي هي في حقيقتها أموال غير نظيفة، وبالتالي فإنهم يحصلون على أموال نظيفة مقابل تلك الودائع، وقد يعلنون عجزهم عن سداد تلك القروض فيتم استيفاء أموال البنك المقترضة من الأموال المودعة.

---

(1) راجع مراد رشدي، مرجع سابق على الشبكة الدولية للمعلومات.

وأكثر من ذلك فقد يتم الاقتراض من بنك في دولة معينة بموجب ضمانة الودائع الموجودة في بنك آخر في دولة أخرى.

كما يمكن لصاحب الأموال المودعة أن يحصل على بطاقة ممغنطة من البنك المودع لديه، يستطيع بموجبها أن يسحب الأموال إلكترونيا من أي مكان في العالم، وغالبا ما يلجأ إلى سحب أمواله عن طريق دول تكون لعملتها قيمة كبيرة مقارنة بالعملات الأخرى، ويستطيع بعد ذلك أن يدخلها في أي مشروع استثماري لأن مصدرها معروف.

ب- التجارة الإلكترونية

وهي ذلك النوع من التجارة التي تتم بواسطة نقل المعلومات بين جهازين للحاسوب الآلي وفقا لقواعد معينة متفق عليها سواء بالنسبة للعرض أم الطلب أم التعاقد أم التنفيذ(1).

ومما لا شك فيه بأن أحد الأساليب المتبعة في غسل الأموال هي وسيلة التجارة الإلكترونية، عن طريق عقد الصفقات المالية الضخمة مع الشركات الكبرى، ثم إعادة طرحها في الأسواق، كصفقات السيارات أو العقارات أو المعادن الثمينة (2)، نظرا لانتشار التجارة الإلكترونية في الآونة الأخيرة ولكون تلك التجارة لا تشترط أن يكون أطراف العقد في المواجهة، ولا يشترط كذلك أن يتم تنفيذ التزام العقد في ذلك المكان.

ومن خلال ما سبق يتضح بأنه لا يوجد ما يمنع من تطبيق نصوص القانون اليمني والجزائري على جريمة تبييض الأموال المرتكبة عبر الإنترنت وبالوسائل الحديثة لمبررات منها:

- لكون تلك النصوص تضمنت الأفعال التي يمكن أن تتم في إطار العالم الرقمي كالتحويلات الإلكترونية للأموال(3)، فجميع العمليات التي يتم بها غسيل الأموال -الإيداع، أو الإخفاء، أو التحويل- يمكن أن تدخل في الجريمة بصورتها المعلوماتية، وما يميز التشريع الجزائري عن اليمني في هذا الشأن هو أنه تناول تعريف الأموال

(1) مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، 2001، ص 10 وما بعدها.
(2) مراد رشدي، مرجع سابق متاح على الشبكة الدولية للمعلومات.
(3) ويقصد بنظام التحويلات الإلكترونية للأموال بأنه: عملية فتح الصلاحية لبنك ما، للقيام بحركات التحويلات المالية الدائنة والمدينة إلكترونيا، عبر الهاتف، وأجهزة الكمبيوتر، وأجهزة المودم عوضا عن استخدام الورق. راجع: سعد غالب ياسين، بشير عباس العلاق، الأعمال الإلكترونية، دار المناهج، عمان- الأردن، 2006، ص296.

التـي يمكـن أن تتعـرض للغسـل، ولـم يفـرق بـين الأمـوال الماديـة والمعنويـة، وكـذلك الأموال المنقولة وغير المنقولة، ولم يحدد وسيلة معينة للحصول على تلك الأموال بل أنـه قد أشـار إلـى أي وسيلة كانـت، وبـأي شكل كانـت تلـك الأمـوال- ومنهـا الصـكوك والوثائق- بما فيها الشكل الالكترونـي أو الرقمـي[1]، ويكـون بـذلك قد سـار علـى نـهج القانون الفرنسي [2].

فجميع العمليات التي يتم بها غسيل الأموال يمكـن أن تـدخل فـي الجريمـة بصـورتها المعلوماتية .

- الجريمـة المرتكبـة بواسـطة الإنترنـت لا تختلـف عـن الجريمـة المرتكبـة بالوسـائل التقليدية سوى في استخدام الوسيلة.
- صـدور قـانون التعـاملات الإلكترونيـة فـي الـيمن كخطـوة فـي مجـال إقـرار التعـاملات التجارية الرقمية – التجارة الإلكترونية – وكما سبق إيضـاح إمكانيـة ارتكـاب جريمـة غسيل الأموال عن طريق التجارة الإلكترونية، فإن تلك الجرائم تخضع لقـانون غسـيل الأموال اليمني طالما تم إقرار المعاملات التي تتم باستخدام التقنية الحديثة.

ومع كل ذلـك فـإن علـى المشـرع اليمنـي الـنص صـراحة علـى تجـريم غسـيل الأمـوال عـن طريـق الإنترنـت، عنـد تعـديل التشـريع مسـتقبلا حتـى لا يكـون هنـاك أي إشـكال فقهـي أو قانونـي يتعلق بـالمسألة أسوة بعدد من التشريعات[3].

---

(1)المادة (4) القانون رقم (05-1)المؤرخ في 6 فبراير سنة 2005 بشأن الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم.

(2) ساير القانون الجزائري القانون الفرنسي في عدم تحديد وسيلة بعينها ترتكب من خلالها عملية غسيل الأموال، أو العمليات التي يتم بها غسل الأموال، فالمشرع الفرنسي قد قرر بأن الجريمة ترتكب بأي وسيلة كانت، وبذلك فإن كافة صور الإخفاء أو التمويه لحقيقة الأموال غير النظيفة أو مصدرها، أو مكانها أو طريقة التصرف فيها، أو حركتها، أو الحقوق المتعلقة بها، أو ملكيتها، جميع تلك الأفعال تدخل في السلوك المادي المكون للركن المادي لجريمة غسيل الأموال بأي وسيلة ارتكب ذلك الفعل أو تلك الأفعال .راجع خلف الله عبد العزيز: جريمة تبييض الأموال، رسالة ماجستير، كلية الحقوق والعلوم الإدارية بن عكنون، 2004،ص50.

(3) نصت المادة (19) من القانون الاتحادي الإماراتي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات على جريمة غسيل الأموال المرتكبة بواسطة التقنية الحديثة ونظم المعلومات بقولها (مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالحبس مدة لا تزيد على سبع سنوات، وبالغرامة التي لا تقل عن ثلاثين ألفاً ولا تزيد على مائتي ألف درهم، كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب وحيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعاً لارتكاب أي من هذه الأفعال)، مرجع سابق على شبكة الإنترنت.

المطلب الثالث

جرائم المخدرات المرتكبة بواسطة الإنترنت

تعد المشاركة الغير مشروعة بين المخدرات وتكنولوجيا المعلومات من أخطر مظاهر التعامل السلبي في مجال تكنولوجيا المعلومات، فالتطور التكنولوجي قد ضاعف من ارتكاب جريمة المخدرات بنسبة كبيرة مقارنةً بارتكابها بالوسائل التقليدية[1]، وقد كان ذلك سببا في تضمين العديد من التشريعات تجريم الترويج والإتجار بالمخدرات عن طريق الإنترنت.

فشبكة الإنترنت تستطيع أن تؤمن فرصاً جديدة وفوائد مضاعفة للأعمال غير الشرعية، نظرا لما توفره من خدمات معلوماتية للمجرمين ليستعملوها لأغراضهم الإجرامية[2]، كون الجانب المظلم من الإنترنت لا يشمل فقط الاحتيال والسرقة ونشر المواد الإباحية، والاتجار بالبشر[3]، بل أن شبكة الإنترنت قد أضحت مستخدمة من قبل منظمات الإتجار بالمخدرات والمنظمات الإجرامية التي تركز على استغلال ما توفره الشبكات من تسهيلات وفرص أكثر لارتكاب جرائم المخدرات، فقد أصبحت قضية بيع

---

(1) حيث يقدر الخبراء عدد مدمني المخدرات بحوالي 320 مليون شخص في أنحاء العالم معظمهم من فئة الشباب، ويكلف الإدمان ما يزيد عن 500 مليون$ سنويا، ويستهلك المدمنون ما يزيد عن 3 الف طن أفيون، و 417 الف طن من مسحوق الكوكايين، و38 الف طن من المارنجونا، و900 الف طن من الحشيش، ولاشك بأن هذه الإحصائيات ستتضاعف بكثير عما هي عليه في ظل استخدام شبكة الإنترنت في التعريف والترويج والإتجار بالمخدرات،والأمثلة على ذلك كثيرة فمثلا في الولايات المتحدة الأمريكية تم ضبط 200موقع على شبكة الإنترنت كانت تستغل في الترويج لهذه الآفة والمتاجرة بها، وفي إحصائية قامت بها إحدى شركات إنتاج البرمجيات الحاسوبية بالولايات المتحدة الأمريكية حول المواقع المشبوهة اكتشفت وجود أكثر من 60 ألف موقع غير ملائمة لأسباب عدة منها التشجيع على تعاطي المخدرات والمؤثرات العقلية بصورة غير مشروعة. لمزيد من التفصيل حول الجريمة والإحصاءات المشار إليها راجع: عبد العزيز العشاوي، ((الجرائم المنظمة بين الجريمة الوطنية والجريمة الدولية))، مجلة كلية أصول الدين للبحوث والدراسات الإسلامية، ع3، سبتمبر2000 ، ص210. وراجع حسين بن سعيد الغافري، الإنترنت وآفة المخدرات، ورقة عمل قدمت لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت الذي انعقد بالقاهرة من 2 إلى4 يونيو2008، منشور على شبكة الإنترنت، ت.د 2009/4/20، على الرابط:

http://www.f-law.net/law/showthread.php?t=28534

(2) محافظي محمود، ((عصر العولمة واستعمال الإنترنت في اختلاس الأموال))، مجلة دراسات قانونية، دار القبة للنشر والتوزيع، الجزائر، ع 5، ديسمبر 2002، ص 58.

(3)وفقا لدراسة جرت برعاية الولايات المتحدة وانتهت عام 2006، تجري المتاجرة بحوالي 800,000 شخص عبر حدود وطنية، وذلك لا يشمل ملايين الأشخاص الذين تجري المتاجرة بهم داخل حدود بلادهم، و 80 بالمائة من الضحايا الذين من خارج البلاد هم نساء وفتيات، وحوالي 50 بالمائة هن من القاصرات، وغالبية الضحايا مم النساء جرت المتاجرة بهن في استغلال جنسي تجاري، وهذه الأعداد لا تشمل ملايين الضحايا من الإناث والذكور حول العالم الذين تجري المتاجرة بهم ضمن الحدود الوطنية لبلادهم. راجع: تقرير وزارة الخارجية الأمريكية لعام 2007 حول الاتجار بالبشر منشور على موقع america.gov، ت.د 2008/1/20 على الرابط:

http://www.america.gov/st/washfile-arabic/2007/June/20070612124835ssissirdile0.5759546.html

وتهريب المخدرات من أسهل ما يمكن من خلال الإنترنت، حيث لا يوجد وسيط بين البائع والمشتري، إذ يمكن للفرد أن يشتري المخدرات مباشرة من خلال الإنترنت، إضافة إلى الدور التي تلعبه الشبكة من خلال بعض المواقع التي تقوم بتعليم الكيفية التي يتم بواسطتها صناعة المخدرات، وزراعتها.

ونظراً لأن جرائم المخدرات عديدة منها الاستعمال الشخصي، والإتجار بها وحيازتها أو تخزينها ووضعها تحت تصرف الغير وزراعتها، وتصنيعها فسيتم تناول أركانها وعقوباتها بإيجاز، ومعرفة مدى تناسب نصوص القانون اليمني والجزائري في مواجهتها.

1. الركن الشرعي لجرائم المخدرات

وردت العديد من المواد في قانون مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية اليمني والجزائري التي تجرم الصور التي ترتكب بها جرائم المخدرات، وهي المواد من (1 إلى 56) من القانون اليمني والمواد من (1 إلى 39) من القانون الجزائري[1]، ومن تلك الصور التي جرمتها تلك النصوص:

- تجريم التعاطي، أو الاستعمال الشخصي.
- تقديم المخدرات للتعاطي، أو تسهيل تعاطيها، أو التواجد في مكان التعاطي.
- إساءة استعمالها في غير الأغراض المخصصة لها.
- جلبها، أو تصديرها، أو نقلها .
- كل الأفعال التي تتعلق بالإتجار بها، سواء التملك، أو الإحراز أو التسليم، أو الزراعة، أو الإنتاج، أو الصناعة.

وتكاد المواد المشار إليها في كلا القانونين أن تكون موحدة، ويبدو ذلك جلياً في التشابه الكبير بين نصوص تلك المواد مع اختلاف بسيط من حيث التقديم أو التأخير أو الصياغة، لكون مصدرها الأساسي هو التشريع الفرنسي مع فارق أن التشريع الجزائري استسقى نصوصه مباشرة من التشريع الفرنسي، بخلاف اليمني الذي غالبا ما تكون

(1) راجع: المواد من (1 إلى 56) من القانون اليمني رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية، والمواد من (1 إلى 39)من القانون الجزائري رقم(04-18) المؤرخ في 25 ديسمبر سنة 2004، يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين، ط1، الديوان الوطني للأشغال التربوية، الجزائر، 2005، ص1 وما بعدها.

نصوصه مستسقاة من القانون المصري والذي بدوره هو الآخر يكون مأخوذا من القانون الفرنسي.

والفارق في النصوص السابقة هو أن القانون الجزائري في تجريمه للمخدرات تدرج من الأدنى للأعلى، فبدأ بجرائم المخدرات التي ترتكب بهدف الاستعمال الشخصي، وانتهى بالجرائم التي تنتهي بقصد الإتجار، وبالتالي فقد تدرج في العقوبة تبعا لذلك، بخلاف التشريع اليمني حيث بدأ بجرائم المخدرات التي تكون بهدف الإتجار وانتهى بالجرائم التي تكون بغرض الاستخدام الشخصي، وبناء على ذلك فيكون التشريع الجزائري قد أتبع الأسلوب الأمثل في التجريم بحيث يبدأ من الجريمة الأدنى وصولا إلى الجريمة الأكثر جسامة وتتدرج العقوبة تبعا لذلك.

ومع أنه يوجد قانون يمني وقانون جزائري يجرمان التعامل في المخدرات سواء من حيث حيازتها، أم الاستخدام الشخصي، أم الإتجار بها، أم زراعتها، إلا أن كلا القانونين لم يتضمنا نصا قانونيا صريحا في لفظه يجرم تلك الجريمة المرتكبة بواسطة الإنترنت كما فعلت العديد من التشريعات الحديثة والتي منها في التشريع المقارن التشريع الفرنسي[1]، ومن التشريعات العربية التشريع السعودي والتشريع الإماراتي[2].

وقد لا يؤاخذ المشرع اليمني على ذلك، لأنه لم يسن قانون لمكافحة الإجرام المعلوماتي، ويمكن مؤاخذته لعدم إصدار تشريع يجرم الجرائم المرتكبة بواسطة تقنية المعلومات بشكل عام بما فيها المخدرات، فإن المشرع الجزائري يؤخذ عليه عدم تضمين النصوص القانونية الخاصة بتجريم المساس بأنظمة المعالجة الآلية للبيانات نصاً قانونياً يجرم الأفعال التي يتم بواسطتها ارتكاب جرائم المخدرات بواسطة الإنترنت مثل الإتجار، وتسهيل تعاطي المخدرات والمؤثرات العقلية، وغسيل الأموال وغيرها حتى لا تكون هناك أي مشكلة قانونية فيما إذا عرضت على القضاء جرائم من هذا النوع.

---

(1) راجع: عمر محمد أبو بكر يونس، مرجع سابق، ص662

(2) تنص الفقرة(4)من المادة السادسة من نظام مكافحة الجرائم المعلوماتية السعودي على أن: (يعاقب بالحبس مدة لا تزيد عن خمس سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أي من الجرائم المعلوماتية الآتية1- ...4- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات والمؤثرات العقلية، أو ترويجها أو طرق تعاطيها، أو تسهيل التعامل بها).

وتنص المادة(18) من القانون الاتحادي الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على أن: (كل من انشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمه،ا أو تسهيل التعامل بهما في غير الأحوال المصرح بها قانونا يعاقب بالسجن المؤقت).

ومع أن القانون الجزائري الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما 2009، قد أدخل سائر الجرائم التقليدية المرتكبة بواسطة نظم المعلوماتية في التجريم بموجب نصوص قانون العقوبات النافذ، إلا أن النص قد جاء عاما، حيث لم يتضمن بعض الأفعال التي تدخل فيها جرائم المخدرات التي ترتكب عن طريق الإنترنت، ومنها إنشاء مواقع تهدف إلى ترويج المخدرات، ونشر معلومات على الشبكة لتعليم الطرق التي يتم بواسطتها تركيب مواد مخدرة باستخدام بعض الوصفات الطبية في الصيدليات، وغيرها من الأفعال ذات الطبيعة التقنية التي يمكن أن ترتكب بها جرائم المخدرات.

وبالتالي وإزاء عدم وجود نصوص في القانون اليمني والجزائري تتناول تجريم الأفعال ذات الطبيعة التقنية التي ترتكب بها جرائم المخدرات والمؤثرات العقلية، فإنه يمكن تطبيق النصوص التقليدية عليها، مع عدم إغفال المشرع في كلا البلدين تضمين النصوص القانونية تعديلا يقتضي النص الصريح على تجريم الأفعال ذات العلاقة بجرائم المخدرات والمؤثرات العقلية والتي يمكن ارتكابها بواسطة تقنية المعلومات، وتشديد العقوبة عما هي عليه في صورتها التقليدية.

2.الركن المادي لجريمة المخدرات

يقوم الركن المادي في جرائم المخدرات والمؤثرات العقلية على عدد من الأفعال تضمنتها نصوص القانونين اليمني والجزائري منها:

- تقديم، أو تسهيل الاستعمال غير المشروع للمواد المخدرة أو المؤثرات العقلية للغير بمقابل أو مجانا، سواء بتوفير المحل لهذا الغرض، أو بأي وسيلة أخرى، وكذلك الأمر بالنسبة لكل من الملاك والمسيرين والمديرين والمستغلين بأية صفة كانت، لفندق أو منزل مفروش أو نزل أو مطعم أو ناد أو مكان عرض أو أي مكان مخصص للجمهور أو مستعمل من الجمهور، الذين يسمحون باستعمال المخدرات داخل هذه المؤسسات أو ملحقاتها أو في الأماكن المذكورة [1].

(1)المادة (35) من ق.ي رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية، والمادة (15) من ق.ج رقم (04-18) المؤرخ في 20 ديسمبر سنة 2004) يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين .

- حيازة أو شراء، أو أنتاج، أو استخراج، أو فصل، أو صنع مواد مخدرة، أو زراعة نبات من النباتات المخدرة، أو حيازتها أو شرائها بقصد التعاطي أو الاستعمال الشخصي..)[1].
- حيازة، أو إحراز، أو شراء، أو تسليم، أو نقل، أو إنتاج، أو استخراج، أو فصل أو صنع مادة مخدرة، أو زراعة نباتا من النباتات المخدرة، وكان بغير قصد الإتجار، أو التعاطي، أو الاستعمال الشخصي وذلك في غير الأحوال المصرح بها قانونا("2).
- تملك، أو حيازة، أو أحرز، أو شراء، أو بيع، أو تسلم ،أو نقل، أو تصدير، أو جلب، أو سمسرة في مواد مخدرة بقصد الإتجار، أو الترويج، أو تقديم للتعاطي مادة مخدرة، بقصد الإتجار فيها بأي صورة، أو تسيير، أو تنظيم، أو تمويل النشاطات المذكورة [3].
- زراعة نبات من النباتات الواردة في الجدول الخامس[4] المرفق بالقانون، أو تصدير، أو جلب، أو حيازة، أو أحرز، أو شراء، أو بيع، أو تسليم، أو نقل نبات من هذه النباتات في أي طور من أطوار نموها هي أو بذورها، وكان ذلك بقصد الإتجار أو الإتجار فيها بأي صورة وذلك في غير الأحوال المصرح بها في هذا القانون[5].
- وضع مخدرات، أو مؤثرات عقلية في مواد غذائية، أو في مشروبات دون علم المستهلكين[6] ، وهذا الفعل تضمنه القانون الجزائري ولم يتضمنه القانون اليمني.
- التواجد في مكان معد أو مهيأ لتعاطي المخدرات مع علمه بذلك[7].

وبشكل عام فإن الركن المادي في جرائم المخدرات والمؤثرات العقلية بمختلف صورها يقوم على العديد من الأفعال التي تختلف من صورة إلى أخرى.

---

(1) راجع: المادة(38) من ق.ي. وكذلك المادة (12) والمادة (13) من ق.ج.
(2) المادة(34) من ق.ي رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية.
(3) المادة : (3) من ق .ي.رقم(3)لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية، والمادة (17) والمادة(18) والمادة (19) من ق.ج رقم (04-18) المؤرخ في 15 ديسمبر سنة 2004) يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين .
(4)تضمن الجدول الخامس المرفق بقانون مكافحة المخدرات والمؤثرات العقلية اليمني بيانا بأنواع النباتات المخدرة التي يحضر زراعتها.
(5) راجع المادة (29) والفقرة(ب) من المادة (34)ق.ي، والمادتين (20، 21) ق.ج.
(6)المادة (14) من القانون رقم (04-18) مؤرخ في 13 ذي القعدة عام 1425 الموافق 20 ديسمبر سنة 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين .
(7) راجع : المادة (40) من القانون اليمني رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية.

فبينما يقوم في جريمة الحيازة والإحراز للمواد المخدرة على أفعال الشراء، والاستخراج، والصنع، والزراعة، فإنه يقوم في جريمة تسهيل وتقديم المخدر للتعاطي على نشاط ايجابي يتمثل في تقديم المخدر للتعاطي حيث تقوم الجريمة بموجبه سواء أعقبه تعاطي أم لا، وقد يقوم بنشاط سلبي وذلك في حالة الامتناع عن القيام بواجب يقتضيه القانون، ومن ذلك امتناع رجل الشرطة عن القيام بواجبه تجاه من يتعاطى مخدر في مكان هو مكلف بمنع تعاطي المخدرات فيه، ولذا فإن تغاضيه عن الفعل هو بمثابة تسهيل لتعاطي المخدر(1).

ويقوم الركن المادي في جريمة إدارة وتهيئة مكان لتعاطي المخدر أو المؤثرات العقلية على كل فعل من شأنه جعل المكان صالحاً لاستقبال رواده لتعاطي المخدر، وبالتالي فإن فعل إعداد الحقن والشيشة وغيرها من الأفعال التي لها علاقة مباشرة بتعاطي المخدر وتتعلق بتهيئة المكان لذلك، تدخل في مكونات الركن المادي للجريمة بخلاف ما يراه البعض من إدخال أفعال التنظيف والإنارة في الإعداد، لأن ذلك فيه إخلال بمعنى التهيئة ولا تتعلق بصورة مباشرة بتعاطي المخدر(2).

وإذا كانت الأفعال السابقة تمثل الركن المادي في جرائم المخدرات المرتكبة بالطرق التقليدية، فإن الركن المادي في جرائم المخدرات المرتكبة بواسطة الإنترنت يقوم على عدد من الأفعال منها:

- الإتجار بالمخدرات والمؤثرات العقلية عن طريق الإنترنت وتتحقق في عرض المواد المخدرة والمؤثرات العقلية في مواقع معينة والتواصل مع العملاء من مختلف الدول، ومن ثم الاتفاق على الكيفية التي تتم بها عملية الشراء والنقل واستلام القيمة، فلقد كان للتطور المذهل في تكنولوجيا الاتصالات الإسهام في تمكين عصابات وتجار المخدرات من الوصول إلى أماكن إنتاجها، كما ساعدهم ذلك التطور في سرعة نقل الأموال المتحصلة من تجارة المخدرات وإدخالها في دورة رؤوس الأموال على مستوى العالم **(3)**.

(1) راجع: مصطفى مجدي هرجه، جرائم المخدرات في ضوء الفقه والقضاء، دار المطبوعات الجامعية، الإسكندرية، 1992، ص 196.
(2) مصطفى مجدي هرجه، مرجع سابق، ص197.
(3) راجع: فهد سلطان محمد أحمد سليمان، مرجع سابق، ص60.

ومن مظاهر تجارة المخدرات عبر الإنترنت إعداد مواقع تتولى عرض الوصفات الطبية للبيع، وهي وصفات طبية تحتوي على أدوية مخدرة، كذلك عن طريق عرض كيفية القيام بإعداد المخدرات عن طريق الوصفات الشعبية بالاستعانة بمواد غذائية تباع في الأسواق، وبمستحضرات طبية تباع في الصيدليات والمستشفيات، حيث تقوم المواقع التي تروج للمخدرات بمثل هذه الأفعال الأخيرة بهدف كسب عملاء جدد والمحافظة على العملاء السابقين الذين لم يعد باستطاعتهم شراء المخدرات لعدم وجود الأموال، فيكون بإمكانهم الحصول على مواد بديلة حتى تتوفر لديهم الأموال(1)، وبالتالي فإن تجار المخدرات يقوموا بتلك الأفعال بغرض المحافظة عل سوق الطلب بل وزيادته.

- بالإضافة إلى جريمة الترويج والإتجار بالمخدرات عن طريق الإنترنت، يمكن ارتكاب جريمة أخرى عن طريق الإنترنت وهي تسهيل تعاطي المخدرات والمؤثرات العقلية، حيث تقوم الجريمة بكافة الأفعال التي تتضمن التعريف بكيفية الحصول على المخدر وكيفية استخدامه والبدائل التي يمكن أن تحل محل المخدرات، فتلك الأفعال يمكن أن تتم عن طرق الإنترنت مثلها مثل الطرق أو الوسائل التقليدية بل إنها تعد أكثر خطورة لأن الإنترنت أصبحت من الوسائل التي اعتاد أغلب الناس على متابعة كل ماهو جديد فيها، وبالتالي فهي سلاح ذو حدين يمكن استخدامه في الخير أو الشر(2).

وما قيل في أركان جريمة المخدرات المادي والمعنوي وفقا للقواعد العامة يمكن أن ينطبق على جريمة المخدرات عن طريق الإنترنت باستثناء التواصل المادي بين تجار ومروجي المخدرات وبين المتعاملين معهم مثلها مثل باقي المنتجات التي يتم الإتجار بها إلكترونيا باستثناء أن هذه التجارة تعد غير مشروعة .

---

(1)عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضة العربية،2004 ، ص661.

(2) الإنترنت من الوسائل التكنولوجية الحديثة التي تسهل عرض المخدرات والمؤثرات العقلية على أكبر شريحة في المجتمع، وذلك بسبب أنها من الوسائل المتاح استخدامها للكافة، بالإضافة إلى الجوانب السلبية للانترنت في مجال الإباحية حيث يعد سببا في كسب أكبر عدد من الشواذ والمارقين عن قيم المجتمع، وبالتالي فإن هذا الجيل الذي تؤثر فيه تلك التكنولوجيا بجانبها السلبي، يصبحوا فيما بعد مهيئون لان يكونوا تحت رحمة عصابات المافيا وتجار المخدرات الذين يجدون منهم ملاذا لاستعمال وترويج منتجاتهم.

3.الركن المعنوي.

يقوم الركن المعنوي لجريمة المخدرات على القصد الجنائي العام بعنصريه العلم والإرادة، بالإضافة إلى القصد الجنائي الخاص في جريمة الإتجار في المخدرات والمؤثرات العقلية.

ويقوم القصد الجنائي العام في جرائم المخدرات على عنصري العلم والإرادة، فيجب أن يكون الجاني عالما بأنه يقوم بفعل من الأفعال التي تقوم بها جريمة الإتجار بالمخدرات، سواءً حيازتها، أم إحرازها، أم تقديمها للتعاطي، أم زراعتها، أم تصديرها، أم استيرادها،أم نقلها، أم صرفها بدون مراعاة الشروط الطبية المنصوص عليها في القانون، أم غير ذلك من الأفعال التي نص عليها القانون اليمني و الجزائري.

كما يجب أن يتوافر عنصر الإرادة إلى جانب عنصر العلم، وذلك حتى يمكن القول بأن الجريمة قد تحققت، فيجب أن تكون الأفعال التي يتحقق بها الركن المادي للجريمة قد تم ارتكابها بإرادة حرة ومدركة لطبيعة الفعل.

وإضافة إلى القصد الجنائي العام ، يجب أن يتوفر القصد الجنائي الخاص في جريمة الإتجار بالمخدرات التي يشترط لقيامها بجانب القصد الجنائي العام أن يكون ذلك بنية الإتجار فيها، بالإضافة إلى تطلب القصد الجنائي الخاص كذلك في جريمة الإحراز أو الحيازة للمواد المخدرة، بحيث يتمثل القصد الجنائي الخاص في أن يكون الإحراز أو الحيازة بنية التعاطي أو الاستعمال الشخصي.

4.العقوبات

1) العقوبات الأصلية والتكميلية في القانون اليمني

أ – العقوبات الأصلية

وفقاً لنصوص القانون اليمني الخاص بمكافحة المخدرات والمؤثرات العقلية، فإن عقوبات جرائم المخدرات تنقسم إلى عقوبات أصلية وعقوبات تكميلية وتتراوح العقوبات الأصلية بين الإعدام والسجن خمس سنوات:

- الإعدام: تطبق عقوبة الإعدام في حالة قيام المتهم بالاستيراد، أو التصدير، أو الإنتاج، أو الاستخراج، أو الفصل للمخدرات والمؤثرات العقلية بقصد الإتجار[1].
- الإعدام أو السجن: تكون العقوبة الإعدام أو السجن لمدة خمسة وعشرين (25)عاما لكل من تملك، أو حاز، أو أحرز، أو اشترى، أو باع، أو سلم، أو نقل، أو قدم للتعاطي مادة مخدرة بقصد الإتجار، وتطبق ذات العقوبة على كل من زرع نباتا من النباتات الواردة في الجدول الخامس، أو صدر، أو جلب، أو حاز، أو أحرز، أو اشترى، أو باع، أو سلم، أو نقل نباتا من هذه النباتات في أي طور من أطوار نموها هي أو بذورها، وكان ذلك بقصد الإتجار، كما تطبق نفس العقوبة على كل من تصرف بالمواد المخدرة خلافا للأغراض التي رخص له باستخدامها، وكذلك لكل من أدار، أو أعد ،أو هيأ مكانا لتعاطي المخدرات، وتطبق العقوبة السابقة على كل من قدم للتعاطي بغير مقابل مواد مخدرة أو سهل تعاطيها، وتطبيق العقوبات المذكورة مشروط بعم الترخيص[2].
- السجن لمدة خمس سنوات: تطبق عقوبة السجن خمس سنوات على كل من حاز، أو اشترى، أو أنتج، أو استخرج، أو فصل، أو صنع، مواد مخدرة، أو زرع نبات من النباتات الواردة في الجدول رقم(5) أو حازها أو اشتراها وكان ذلك بقصد التعاطي أو الاستعمال الشخصي، وتطبق نفس العقوبة على كل من حاز، أو أحرز، أو اشترى، أو سلم، أو نقل، أو أنتج، أو استخرج، أو فصل، أو صنع مادة مخدرة، أو زرع نباتا من النباتات الواردة في الجدول رقم(5) وكان بغير قصد الإتجار أو التعاطي أو الاستعمال الشخصي وذلك في غير الأحوال المصرح بها قانونا[3].
- الحبس مدة سنة: لكل من ضبط في أي مكان أعد، أو هيأ لتعاطي المخدرات وكان يجري فيه تعاطيها مع علمه بذلك، ولا ينطبق هذا الحكم على الزوج أو الزوجة أو أصول أو فروع او إخوة أو أخوات من أعد أو هيأ المكان المذكور[4].

---

(1) المادة (33) من القانون رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية.

(2) المادة رقم (34) والمادة رقم (35) من القانون رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية.

(3) المواد (38 و 39) من القانون رقم (3) لسنة 1993 من نفس القانون.

(4) المادة رقم 40 من نفس القانون.

ب - العقوبات التكميلية

- مصادرة الأموال المتحصلة من جرائم المخدرات أيا كان نوعها.
- مصادرة المواد المخدرة، أو النباتات المضبوطة الوارد ذكرها في الجدول رقم(5) وإتلافها بنظر السلطة القضائية المختصة، وكذلك مصادرة الأدوات ووسائل النقل التي تكون قد استخدمت في ارتكاب الجريمة وتخصص الأدوات ووسائل النقل المحكوم بمصادرتها لصالح الجهة التي تولت ضبطها.

2) العقوبات الأصلية والتكميلية في القانون الجزائري

عقوبة جرائم المخدرات في القانون الجزائري بدأت من الأدنى إلى الأعلى حسب ترتيب النصوص القانونية، بداية بالحبس من شهرين إلى سنتين وانتهاءً بالسجن المؤبد لبعض الجرائم.

أ- العقوبات الأصلية

- تكون عقوبة جريمة الحيازة للاستهلاك الشخصي: الحبس من شهرين (2) إلى سنتين(2)وغرامة من 5.000 د.ج إلى 50.000 د.ج أو بإحدى هاتين العقوبتين[1].

- وتكون عقوبة العرض أو التسليم للغير للاستهلاك الشخصي :" الحبس من سنتين (2) إلى عشر(10) سنوات وغرامة من 100.000 دج إلى 500.000دج. ويضاعف الحد الأقصى للعقوبة إذا تم تسليم أو عرض المخدرات والمؤثرات العقلية على قاصر، أو معوق، أو شخص يعالج بسبب إدمانه، أو في مراكز تعليمية، أو تربوية، أو تكوينية، أو صحية، أو اجتماعية، أو داخل هيئات عمومية"[2].
- كما جعل القانون عقوبة إعاقة، أو عرقلة المكلفين بمعاينة هذا النوع من الجرائم: الحبس من سنتين(2) إلى خمس(5)سنوات والغرامة من100.000 دج إلى 200.000 دج [3].

(1) راجع: المادة (12) من القانون الجزائري رقم (04-18) المؤرخ في 13 ذي القعدة عام 1425 الموافق 20 ديسمبر سنة 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين.
(2) المادة(13) من القانون الجزائري رقم (04-18 مؤرخ في 13 ذي القعدة عام 1425 20 ديسمبر سنة 2004) يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين.
(3) المادة (14)من نفس القانون.

- وعقوبة تسهيل تعاطي المخدرات والمؤثرات العقلية: الحبس من خمس(5) سنوات إلى خمس عشرة(15)سنة وبغرامة من 500.000 دج إلى 1000.000 دج [1].
- بينما تكون عقوبة تقديم وصفة طبية صورية أو على سبيل المحاباة، أو تسليمها بدون وصفة: الحبس من خمس(5) سنوات إلى خمس عشرة(15)سنة وغرامة من 500.000 دج إلى 1000.000 دج [2].
- وجعل المشرع الجزائري عقوبة الأفعال التي تتعلق بالإتجار:الحبس من عشر(10) سنوات إلى عشرين(20) سنة وغرامة من 5000.000 دج إلى 50.000.000 دج لكل من قام بطريقة غير مشروعة بإنتاج، أو صنع، أو حيازة، أو عرض، أو بيع، أو وضع، للبيع، أو حصول، أو شراء قصد البيع أو التخزين، أو استخراج، أو تخزين، أو تحضير، أو توزيع، أو تسليم بأية صفة كانت، أو سمسرة أو شحن، أو نقل عن طريق العبور، أو نقل المواد المخدرة والمؤثرات العقلية .
- **السجن المؤبد** لكل من قام بإنتاج، أو صنع، أو حيازة، أو عرض، أو بيع، أو وضع، للبيع أو حصول أو شراء قصد البيع أو التخزين، أو استخراج، أو تخزين، أو تحضير، أو توزيع، أو تسليم بأية صفة كانت أو سمسرة أو شحن أو نقل عن طريق العبور أو نقل المواد المخدرة والمؤثرات العقلية **-**الأفعال المرتبطة بالإتجار والترويج للمخدرات – وكان ضمن عصابة إجرامية منظمة.
- كذلك تكون عقوبة السجن المؤبد لكل من **قام** بتسيير أو تنظيم أو تمويل النشاطات السابقة، أو قام بتصدير أو استيراد مخدرات أو مؤثرات عقلية، أو زرع بطريقة غير مشروعة خشخاش الأفيون، أو شجيرة الكوكا، أو نبات القنب، أو قام بصناعة، أو نقل، أو توزيع سلائف أو تجهيزات أو معدات، إما بهدف استعمالها في زراعة المواد المخدرة أو المؤثرات العقلية، أو في إنتاجها أو صناعتها بطريقة غير مشروعة، وإما مع علمه بأن هذه السلائف أو التجهيزات أو المعدات ستستعمل لهذا الغرض.

---

(1) المادة (15) من القانون الجزائري رقم (04-18) المؤرخ في 13 ذي القعدة عام 1425 الموافق 20 ديسمبر سنة 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين
(2) المادة (16)من نفس القانون.

- ويعاقب كل من يحرض، أو يشجع، أو يحث بأية وسيلة كانت على ارتكاب الجرائم المنصوص عليها في هذا القانون، بالعقوبات المقررة للجريمة أو الجرائم المرتكبة[1].
- يعاقب على الشروع في هذه الجرائم بالعقوبات ذاتها المقررة للجريمة المرتكبة **[2].**
- يعاقب الشريك في الجريمة أو في كل عمل تحضيري منصوص عليه في هذا القانون بعقوبة الفاعل الأصلي[3].
- يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في المواد من 13 إلى 17 من هذا القانون بغرامة تعادل خمس(5) مرات الغرامة المقررة للشخص الطبيعي .
- يعاقب الشخص المعنوي بغرامة تتراوح من 50.000.000 دج إلى 250.000.000 دج.
- في جميع الحالات، يتم الحكم بحل المؤسسة أو غلقها مؤقتاً لمدة لا تفوق خمس (5)سنوات .

ب- العقوبات التكميلية

- المنع من ممارسة المهنة التي ارتكبت الجريمة بمناسبتها لمدة لا تقل عن خمس(5) سنوات.
- المنع من الإقامة وفقا للأحكام المنصوص عليها في قانون العقوبات.
- سحب جواز السفر وكذا سحب رخصة السياقة لمدة لا تقل عن خمس(5)سنوات.
- المنع من حيازة أو حمل سلاح خاضع للترخيص لمدة لا تقل عن خمس(5) سنوات.
- مصادرة الأشياء التي استعملت أو كانت موجهة لارتكاب الجريمة أو الأشياء الناجمة عنها.
- الغلق لمدة لا تزيد عن عشر(10) سنوات بالنسبة للفنادق أو المنازل المفروشة أو مراكز الإيواء والحانات والمطاعم والنوادي وأماكن العروض، أو أي مكان مفتوح

---

(1) راجع: المواد (من17 إلى 22) من ق.ج رقم (04-18) المؤرخ 15 ديسمبر سنة 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين.
(2) المادة(17) من نفس القانون .
(3)المادة(23) من نفس القانون.

للجمهور، حيث ارتكب المستغل أو شارك في ارتكاب الجرائم المنصوص عليها في المادتين:(15، 16)من هذا القانون، ويلاحظ على العقوبات التكميلية في القانون اليمني والجزائري بأنها لم تتضمن عقوبة غلق الموقع الذي يستخدم في ترويج المخدرات مما يؤكد الحاجة إلى تعديل النصوص القانونية وتضمينها مثل هذه العقوبات التي يجب أن تتزامن مع الأفعال الإجرامية ذات الطابع التقني.

المطلب الرابع

جريمة الإرهاب في مجال المعلوماتية

لازال الإرهاب محل خلاف وجدل بين الاتجاهات المختلفة، حيث لم يوضع له تعريف جامع مانع يكون محلاً للإجماع، فما يعد إرهابا في نظر البعض قد يعد عملا مشروعا في نظر البعض الآخر[1]، وقد يرجع السبب في ذلك إلى أن مصطلح الإرهاب مصطلح مازال غير واضح لم يتم الاتفاق على تعريفه بشكل دقيق[2]، لكون بعض الدول تنحو منحىً سياسياً في تعريفه بما يتماشى مع مصالحها حتى لو استهدفت مصالح الآخرين، إضافة إلى أن أحداث 11 سبتمبر 2001م، وكذلك التطور السريع في مجال التكنولوجيا الحديثة وعلى وجه الخصوص تكنولوجيا المعلومات، والتي ظهر بظهورها نوع جديد من الإرهاب هو الإرهاب الالكتروني، كل ذلك قد جعل من المصطلح مصطلحا غامضا.

ففي عصر التطور الرقمي تغيرت معه أشكال الأشياء وأنماطها، ومنها أنماط الجريمة، والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق

([1]) عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008، منشور على موقع منتدى كلية الحقوق- جامعة المنصورة، ت.د 2009/4/10 على الرابط: http://www.f-law.net/law/showthread.php?t=28535

(2) نظرا لعدم وجود تعريف دقيق للإرهاب في أغلب التشريعات التي نصت عليه، فإنه يختلف من دولة إلى أخرى، ومع أنه قد تم عقد العديد من الاتفاقيات الدولية لمكافحة الإرهاب، إلا أن الغموض مازال يكتنف ذلك النوع من الإجرام، فقد يطلق على منظمات معينة أنها منظمات إرهابية، بالرغم من أنها لا تقوم بأعمال إرهابييه، بل إن أعمالها قد تكون من باب المقاومة المشروعة، وبالمقابل فلا يتم إدخال دول أو كيانات ضمن قائمة الإرهاب بالرغم من أعمال التعذيب والتقتيل والتدمير واحتلال الأرض التي تتم بصورة إرهاب دولة، فأين يكمن الإرهاب في ظل هذه التناقضات.

ارتكابها، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب الإلكتروني،والتي أخذت أشكالاً حديثة تتماشى مع التطور التقني[1].

ومع ذلك فيمكن تعريفه بأنه: القيام ببث الرعب والفزع لدى الآمنين، بأية وسيلة كانت، وبما ينذر بعواقب وخيمة في الأرواح أو الممتلكات.

كما ينصرف الإرهاب إلى الأفعال الإجرامية الهادفة إلى إثارة الرعب العام لدى شخصيات معينة، أو مجموعة من الأشخاص، أو الوسط العام[2].

ويعرف الإرهاب الالكتروني(Cyber terrorism): بأنه تعبير يشمل مزج مصطلح التهديد بنظم المعالجة الآلية للمعطيات باستخدام تقنية الاتصالات الحديثة[3].

كما يعرف الإرهاب الالكتروني أيضا: بالتهديد والتخريب التقني لمحطات التحكم وقواعد المعلومات، وأجهزة الحاسوبات، وشبكات الاتصالات والذي ينتج عنه أضرار بالغة وكبيرة[4].

ويتلاقى الإرهاب مع الجريمة المنظمة في أن الجريمتين يشيعان الخوف والرعب لدى المواطنين العزل، كما يتشابهان في شكل تنظيمهما وأساليب تنفيذهما[5].

وينقسم الإرهاب إلى قسمين:

الأول : إرهاب داخلي يقع داخل الدولة.

---

(1) محمد محمد الألفي، جرائم التجسس والإرهاب الإلكتروني عبر الإنترنت، جريدة 26 سبتمبر اليمنية، الاثنين، 16 يناير،2006،على الربط:

http://www.26sep.net/news_details.php?lng=arabic&sid=12133

(2)المادتان (1، 2) من اتفاقية جنيف لعام 1937 المتعلقة بالمنع والقمع الدولي للإرهاب، مشار إليهما لدى عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق.، ص648. كما تجدها منشورة على شبكة المعلومات الدولية، ت.د2009/10/2، على الرابط:

https://www.unodc.org/tldb/pdf/Guide_Terr_Incorporation_Implementation_Ar.doc

(3) Cyber terrorism –Testimony before the U.S. House of Representatives By :Dr. Dorothy E. Denning / Georgetown Uni. May 23 ,2000 . Available on line in 4/10/2009.

http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

(4) سامي الحربي، الإرهاب الالكتروني هل هو حقيقة أم خيال، جريدة الرياض، ع -13449، الأربعاء 11 ربيع الأول 1426هـ الموافق20 إبريل 2005م، وتم التأكد من المعلومات مازالت متاحة في4/ 2009/9 على الرابط:

.http://www.alriyadh.com/2005/04/20/article57983.html

(5) عبد العزيز العشاوي، مرجع سابق، ص213.

والثـاني: إرهـاب دولـي ويشـمل نـوعين مـن الإرهـاب، إمـا إرهـاب دولـي بـالمعنى الكامل حيث يشترط لوقوعه توافر ركن الدولة، وإما أن يكون إرهاب دولي عابر للحدود وهو إرهاب ذو طبيعة دولية إلا أنه يرتكب عن طريق الفرد ويمس كيان الدولة [1].

وتكـاد تجمـع الاتجاهـات الفقهيـة الحديثـة بـأن جريمـة الإرهـاب مـن الجـرائم التـي لا يمكن حصرها في جرائم معينة، لذلك فهي تخضع للتوصـيف القـانوني أو تفسـير القـانون بكـل دولـه علـى حـدة وفقـا لاعتبـارات معينـة[2].وسـيتم تنـاول صـور الجريمـة وأركانهـا وعقوباتها.

1. صور جريمة الإرهاب

تتعدد صور جريمة الإرهاب، سوءاً وردت تحت مسمى الإرهاب كما في عدد من القوانين منها القانون الجزائري، أم تحت مسميات أخرى كما في قوانين أخرى منها القانون اليمني، وسيتم الإشارة إلى تلك الصور على وجه الإجمال حيث سيتم توضيحها بصوره أكثر تفصيلا أثناء تناول الركن لمادي للجريمة.

أ- صور جريمة الإرهاب في القانون اليمني[3].

1- الاعتداء على استقلالية الجمهورية.

2- الاعتداء على الدستور والقانون.

3- العصيان المسلح.

4- الاشتراك في عصابة مسلحة.

5- إذاعة إخبار بغرض تكدير الأمن العام.

6- الحريق والتفجير للأموال الثابتة أو المنقولة.

7- تعريض وسائل النقل والمواصلات للخطر.

8- حيازة المفرقعات والإتجار فيها.

---

(1) عمر محمد أبو بكر يونس، مرجع سابق ، ص647.

(2) راجع: سليم مرحالي، مفهوم الإرهاب في القانون الدولي، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر، 2002/2001، ص51.

(3) تضمن قانون العقوبات اليمني رقم 13 لسنة 1994صور جرائم الإرهاب من خلال نصوص المواد (125، 131، 133، 136، 137، 138، 144، 306، 307، 308).

9- الحرابة[1].

ب- صور الجريمة وفقا للقانون الجزائري[2]

1- الجرائم الماسة بأمن الدولة والوحدة الوطنية واستقرار المؤسسات.

2- إنشاء وتسيير أو الانخراط في الجمعيات والمنظمات والجماعات الإرهابية.

3- التمويل والإشادة وتشجيع الأعمال الإرهابية.

4- جريمة حيازة أو حمل أو استعمال أو المتاجرة في الأسلحة والذخائر والمفرقعات.

5- إلقاء الخطب من غير المعينين بذلك أو مخالفة الخطبة لمهمة المسجد.

والصور سالفة الذكر تكاد تتشابه في القانون اليمني والجزائري، إلا أنها في الجزائري أتت تحت مسمى جرائم الإرهاب، بخلاف اليمني الذي وردت فيه تحت مسميات عديدة منها المساس بأمن الدولة الداخلي، ومنها العصيان المسلح ،وتكدير الأمن العام، وحيازة المواد المتفجرة والإتجار بها بدون ترخيص، وجريمة الحرابة بشكل عام والتي تكاد أفعالها أن تحدث آثاراً من شأنها تخويف الآخرين وترويعهم.

2. أركان جريمة الإرهاب

جريمة الإرهاب كغيرها من الجرائم يتطلب لقيامها تحقق الركن المادي الذي يقوم على الأفعال المكونة للجريمة، وكذلك الركن المعنوي بعنصرية العلم والإرادة، وقبل ذلك لابد أن تكون تلك الأفعال داخلة في إطار التجريم بموجب نصوص قانونية وهو ما يسمى بالركن الشرعي للجريمة:

أ. الركن الشرعي لجريمة الإرهاب

لم يتضمن ق.ع.ي نصوص قانونية صريحة في لفظها تعني بتجريم الأفعال الموصوفة بالإرهابية، إلا أنه عند مقارنتها بنصوص ق.ع الجزائري و ق.ع المصري

---

(1) يقصد بالحرابة كل الأفعال التي يتم من خلالها السطو على الممتلكات وأخذ المال بالقوة، وقد تصل إلى درجة أخذ المال وقتل النفس، وقد تقتصر على القتل دون أخذ المال، إذا حال بين الجاني أو الجناة ما يحول دون ذلك، لذلك جعلتها الشريعة الإسلامية من جرائم الإفساد في الأرض وقررت لها عقوبة تتناسب مع جسامة الجريمة.

(2) راجع: المواد (من 87 مكرر إلى 87 مكرر10).من الأمر رقم(95-11) المؤرخ في 25 فبراير 1995 والذي تم تعديل بعض نصوصه من خلال القانون رقم (06-23) المؤرخ في 20 ديسمبر .2006 ، حيث وردت تلك النصوص تحت مسمى الجرائم الموصوفة بأفعال إرهابية أو تخريبية.

يلاحظ بأنها قد تضمنت الجرائم نفسها التي وردت بالقانونين المذكورين مع عدم ذكر لفظ الإرهاب(terror)[1].

فقد تضمن ق.ع.ي تجريمها تحت مسميات أخرى وفقا لعدد من النصوص ومنها المواد (125، 132، 136، 138، 144، 306، 307، 308)

حيث جرمت المادة (125) كل فعل من شأنه الاعتداء على استقلالية الجمهورية اليمنية، وجرمت المادة (132) إثارة عصيان مسلح أو حرب أهلية، كما جرمت المادة: (136) إذاعة أخبار كاذبة بغرض تكدير الأمن العام، وكذلك فقد جرمت المادة (138) تعطيل وسائل المواصلات والاتصالات بأي وسيلة تم ارتكابها مما يدخل وسائل التكنولوجيا الحديثة في إطار التجريم، كما جرمت المادة (144) الإتجار بالمفرقعات، أما المواد(306، 307، 308) فقد جرمت كل عمل من شأنه التعرض للناس بالقوة لتخويفهم وإرعابهم بقصد أخذ المال أو قتل النفس أو هتك العرض، أو لأي غرض غير مشروع.

كذلك فإن المواد: (من 87مكرر إلى 87مكرر7)من ق.ع.ج. قد تضمنت الركن الشرعي لجريمة الإرهاب، حيث جرمت تلك المواد كل ما من شأنه المساس بأمن الدولة والوحدة الوطنية، وكذلك تسيير أو الانخراط في الجمعيات والجماعات الإرهابية، أو تمويلها، أو الإشادة بها، أو حيازة أو حمل أو الإتجار في الأسلحة والذخائر والمفرقعات، أو إلقاء الخطب التي تدعم أو تشيد بالإرهاب.

ومن خلال الاطلاع على نصوص المواد المشار إليها يلاحظ بان ق.ع.ي لم يتناول الجرائم سالفة الذكر تحت مسمى الإرهاب مثل القانون الجزائري، وإنما تناولها تحت مسميات أخرى وفي فصول متفرقة في القانون، وبالتالي فلا يكون أمام المشرع اليمني إلا الإبقاء عليها مثلما هي بمسمياتها طالما أن النتيجة في النهاية واحدة وهي العقاب على ذات الأفعال التي توصف في قوانين أخرى بالإرهاب، فالمشكلة ليست في التسمية طالما والغرض واحد وهو الوقاية من تلك الجرائم ومعاقبة مرتكبيها.

(1)عالج المشرع المصري جرائم الإرهاب في ق.ع رقم (97) لسنة 1992في الباب الثاني من القسم الأول بعنوان، الجنايات والجنح المضرة بالحكومة من جهة الداخل، وذلك من خلال المواد من (86 وحتى 102) وهي الجرائم التي نص المشرع المصري فيها صراحة على الجرائم الإرهابية.راجع: أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص145.

أمـا إذا أراد أن يطلـق عليهـا مصـطلح جـرائم الإرهـاب، فهـو بحاجـة إلـى تعـديل النصوص القانونيـة وإضـافة اللفظ إلـى الجـرائم المنصـوص عليهـا فـي ق.ع، مثلمـا عمـل المشرع الجزائري.

ويستحسن طالما يوجد مشروع قانون لمكافحـة غسيل الأمـوال ومكافحـة الإرهـاب مطروح على المجلس التشريعي- أن يدرس بعناية و يتم تضمينه النصوص القانونية التي تجعل القانون يتعامل مع الجريمة فـي صـورتها التقليديـة، مـع عـدم إغفـال تلـك النصـوص لعقوبة الجريمة التي ترتكب بوسائل التقنية الحديثة(1).

كما يلاحظ على نصوص ق.ع.ج بأنه قد تضمن تجريم الإرهاب بمختلف صـوره، ويمكن تطبيق تلك النصوص على اقتراف جرائم الإرهاب الرقمي- باستخدام التكنولوجيا الرقمية – كون تلك الجرائم يمكن اقترافها بواسطة الإنترنت، فتشجيع الأعمال الإرهابيـة تعـد مجرمـة بموجـب نـص المـادة (87 مكـرر4)بـأي وسـيلة كانـت ممـا يـدخل الوسـائل الحديثة في نطاق التجريم.

كما أن نص المادة (2) من القانون رقم (09- 04) المؤرخ في 5غشت(أغسطس) يتضـمن الوقايـة مـن الجـرائم المتصـلة بتكنولوجيـات الإعـلام والاتصـال ومكافحتهمـا، قـد ضمن الجرائم التقليديـة التـي ترتكـب أو يسـهل ارتكابهـا عـن طريـق الوسـائل الإلكترونيـة ضمن الجرائم التي تخضـع للقـانون، إضـافة إلـى جـرائم المسـاس بأنظمـة المعالجـة الآليـة للمعطيــات المنصــوص عليهــا فــي قــانون العقوبــات، وبالتــالي فــإن إدارة أو تســيير أو الانخراط في الجمعيات أو المنظمات الإرهابية، أو نشر الوثائق المتعلقة بأفعـال إرهابيـة،

(1) يوجد مشروع قانون يمني لمكافحة غسيل الأموال وتمويل الإرهاب تم تقديمه من قبل الحكومة إلى البرلمان، وتم إحالة المشروع إلى لجنة الدفاع والأمن، واللجنة الدستورية، ولجنة تقنين أحكام الشريعة الإسلامية لدراسته، وقد تضمن عدداً من الجرائم التي وردت في قانون العقوبات، وتتعلق بالمساس بالأمن الداخلي للدولة، أو باستقلال الجمهورية اليمنية، أو وحدة أراضيها، أو تكدير الأمن والسلم الاجتماعي، ومن تلك الأفعال الاختطاف، أو التقطع، أو نهب الأموال والممتلكات العامة بالقوة، أو الاعتداء على المنشآت العامة أو التابعة للشركات الاستثمارية، أو النفطية، وغيرها، وجرم المشروع جمع أو تقديم أموالا بشكل مباشر، أو غير مباشر لاستخدامها في تمويل الأفعال التي لها علاقة بالإرهاب ومنها أعمال العنف التي تثير الرعب والخوف بالمجتمع، وكذلك تمويل الأفعال التي تدخل في جرائم الاختطاف والتقطع، وكذلك تمويل الأفعال التي تشكل جرائم منصوص عليها بالاتفاقيات الدولية الموقعة عليها الجمهورية اليمنية، أو التي تكون طرفا فيها، ومع أن المشروع قد تضمن لفظ الإرهاب، إلا أنه ومن خلال تسمية القانون بقانون مكافحة غسيل الأموال وتمويل الإرهاب، فإن اللفظ ينصرف إلى مكافحة تمويل الإرهاب وليس مكافحة جرائم الإرهاب، مع أن المشروع في صياغة مواده يتضمن مكافحة جرائم الإرهاب وكذلك تمويلها، كما أن المشروع قد تضمن ارتكاب جرائم التمويل بأي وسيلة كانت، مما يوحي بشمول اللفظ على الوسائل الإلكترونية، إلا أن اللفظ اقتصر على التمويل، ولم يشر إلى ارتكاب جرائم الإرهاب عن طريق التكنولوجيا الرقمية، ويجب التنبه لمثل ذلك أثناء إعداد القانون بصيغته النهائية، من حيث التسمية والتطرق من خلال ألفاظ صريحة للجرائم المرتكبة بواسطة الإنترنت، وتكنولوجيا المعلومات.

أو المتاجرة بالأسلحة جميعها يمكن أن ترتكب من خلال الإنترنت، وتبعا لذلك يتعين أن تخضع لنصوص تلك المواد، حيث أن سلاح الإرهاب في ظل تكنولوجيا المعلومات عبارة عن: مجموعة من البرمجيات تجعل الأمر أكثر خطورة مما لو كان الأمر يتعلق بأسلحة أخرى، وعلى سبيل المثال يمكن الحصول على المعلومات الضرورية في تطوير الأسلحة الكيماوية والبيولوجية عن طريق الإنترنت (1).

ومع ذلك فإن القانون الجزائري وكذلك اليمني لم يتضمنا تجريم بعض الأفعال ذات العلاقة بالتقنية الرقمية مثل تجريم مجرد إنشاء موقع، أو مواقع تتبع تنظيمات إرهابية، أو النص بشكل صريح وتشديد العقوبة على جريمة الإرهاب التي تقترف بواسطة تكنولوجيا الإعلام والاتصال، وكذلك الإرهاب الإلكتروني الذي يتم عن طريق أفعال تقنية تتسبب في تعطيل المنشآت الهامة أو الخدمات التي تدار إلكترونيا، أسوة بالتشريعات الحديثة ومنها في المقارن التشريع الفرنسي(2)، وفي التشريعات العربية التشريع السعودي والتشريع الإماراتي، حيث نصا على عقوبات لجريمة الإرهاب التي تقترف بواسطة تكنولوجيا المعلوماتية، مثل أنشاء مواقع تتبع منظمات إرهابية، أو نشر بيانات تتبناها جماعات إرهابية يتم من خلالها تعليم صناعة المتفجرات أو استخدامها، وغير ذلك من الأفعال ذات العلاقة بالإرهاب المعلوماتي (3).

---

(1) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص658.

(2) Art.(421-1- CPN FR)...(Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes : …2- Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code;)(art.323-1 et s.).
http://www.legislationline.org/upload/legislations/cd/1b/f05864013134135c992550ab7c98.htm.
وراجع أيضاً : عمر محمد أبو بكر يونس، الجرائم الناشئة عن الإنترنت، مرجع سابق، ص651.

(3) نصت الفقرة(1)من المادة السابعة من نظام مكافحة الجرائم المعلوماتية السعودي على أن (يعاقب بالسجن مدة لا تزيد عن عشر سنوات وبغرامة لا تزيد عن خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية التالية: إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسوب الآلي أو نشره، لتسهيل الإتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية).
ونصت المادة: (21)من القانون الإماراتي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على: (كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات).

ب. الركن المادي لجريمة الإرهاب

تتعدد الأفعال التي يتكون منها للركن المادي في جريمة الإرهاب باختلاف الصور التي تتضمنها تلك الجريمة :

1) الاعتداء على استقلالية الجمهورية

لم يحدد المشرع اليمني أفعالا بذاتها لقيام الجريمة، ولذلك فإن أي فعل يتم ارتكابه بقصد المساس باستقلال الجمهورية أو وحدتها أو سلامة أراضيها يشكل الركن المادي للجريمة،[1].

وذلك بخلاف القانون الجزائري الذي وضح الأفعال التي تكون الركن المادي لهذه الجريمة، تحت مسمى الجرائم الماسة بأمن الدولة والوحدة الوطنية واستقرار المؤسسات، أو تمويل، أو الإشادة، أو تشجيع تلك الأفعال الإرهابية، أو نشرها، أو إعادة طباعة الوثائق والتسجيلات التي تشيد بتلك الأعمال.

حيث نصت المادة: (87 مكرر) ع.ج على أن (يعتبر فعلا إرهابيا أو تخريبيا، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يلي :

- بث الرعب في أوساط السكان، وخلق جو انعدام الأمن، من خلال الاعتداء المعنوي والجسدي علي الأشخاص أو تعريض حياتهم وحرياتهم وأمنهم للخطر، أو المساس بممتلكاتهم.
- عرقلة حركة المرور، أو حرية النقل في الطرق، أو التجمهر، أو الاعتصام في الساحات العمومية.
- الاعتداء على رموز الأمة والجمهورية، ونبش أو تدنيس القبور.
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة، والاستحواذ عليها أو احتلالها دون مسوغ قانوني.
- الاعتداء على المحيط، أو إدخال مادة أو تسريبها في الجو، أو في باطن الأرض، أو إلقائها عليها، أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.

---

(1) راجع المادة (125) من ق.ع .ي رقم 12لسنة 1994.

- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة أو الحريات العامة وسير المؤسسات المساعدة للمرفق العام.
- عرقلة سير المؤسسات العمومية، أو الاعتداء على حياة أعوانها أو ممتلكاتهم، أو عرقلة تطبيق القوانين والتنظيمات)(1).

وتضمنت(87 مكرر4) ع.ج أفعال الإشادة أو الدعم للأفعال المذكورة أنفا - في المادة(87 مكرر)- أو تشجيعها أو تمويلها بأي وسيلة كانت(2).

وكذلك فقد تضمنت المادة(87 مكرر 5) ع.ج على عقوبة من يعيد طبع، أو نشر الوثائق التي تشيد بالأفعال الإرهابية (3).

وبالتالي فإن الركن المادي وفقا لنص القانون الجزائري يقوم في هذه الجريمة على أي فعل من شأنه استهداف أمن الدولة، والوحدة الوطنية، والسلامة الترابية، واستقرار المؤسسات وسيرها العادي بغرض بث الرعب في وسط المجتمع، وتخويفهم وترهيبهم بالاعتداء المعنوي والجسدي عليهم، وتعريض أمنهم وحرياتهم، والمساس بممتلكاتهم وعرقلة حرية التنقل في الطرق وعمل السلطات والمؤسسات العمومية

2) الاعتداء على الدستور والقانون

ويتكون الركن المادي في هذه الصورة من صور الإرهاب بفعل التوصل، أو الشروع في التوصل بالعنف أو التهديد أو أية وسيلة أخرى غير مشروعة إلى:

- إلغاء أو تعديل أو إيقاف الدستور أو بعض نصوصه.
- تغيير أو تعديل تشكيل السلطة التشريعية أو التنفيذية أو القضائية أو منعها من مباشرة سلطاتها الدستورية أو إلزامها باتخاذ قرار معين(4).

---

(1)المادة 87 مكرر من الأمر (رقم 95- 11) المؤرخ في 25فبراير 1995المُعَدِل والمُتَمِمْ للأمر رقم (66- 156) المؤرخ في 8يونيو 1966يتضمن قانون العقوبات، والفارق بين النص في القانون اليمني وهذا النص هو: أن الجريمة في الجزائري وردت تحت عدد من الأفعال الموصوفة بالإرهاب، بخلاف اليمني –المادة(125)- حيث وردت تحت مسمى الجرائم الماسة بأمن الدولة ووحدتها وسلامة أراضيها.
(2) المادة (87 مكرر4) من (الأمر رقم 95-11 المؤرخ في 25 فبراير 1995) المُعَدِل والمُتَمِمْ للأمر رقم (66-156) المؤرخ في 8يونيو 1966يتضمن قانون العقوبات.
(3) والأفعال الإرهابية التي أشار إليها النص هي الأفعال التي تم ذكرها وتضمنتها المادة (87 مكرر). راجع المادة (87 مكرر) والمادة(87 مكرر5) من الأمر رقم 95-11 المؤرخ في 25 فبراير 1995.
(4) راجع : المادة(131) من ق.ع.ي رقم 12 لسنة 1994.

3) جريمة العصيان المسلح

تضمنت الفقرات (5)و(6) و(7) من المادة (132) بعض الأعمال التي يمكن اعتبارها إرهابية بالنظر إلى ما تحدثه في المجتمع من تخويف وترهيب، ومن تلك الأفعال إثارة أو الشروع في إثارة عصيان مسلح لدى الناس ضد السلطات القائمة بموجب الدستور، وكذلك إثارة أو الشروع في إثارة حرب أهلية عن طريق توزيع السلاح على طائفة من السكان أو الدعوة إلى حمله لاستعماله ضد طائفة أخرى، كذلك يتحقق الركن المادي في هذه الصورة بالتحريض على ارتكاب جرائم القتل أو النهب أو الإحراق[1].

4) الاشتراك في عصابة مسلحة

وفي هذه الصورة من صور جرائم الإرهاب يتحقق الركن المادي بتحقق الأفعال التالية:

- الإشتراك في عصابة مسلحة بقصد اغتصاب الأراضي أو نهب الأموال المملوكة للدولة أو لجماعة من الناس، أو مقاومة القوة العسكرية المكلفة بمطاردة مرتكبي هذه الجرائم.
- الإشتراك في عصابة مسلحة لمهاجمة جماعة من الناس أو مقاومة رجال السلطة العامة المكلفين بتنفيذ القوانين.

5) إذاعة إخبار بغرض تكدير الأمن العام

ويتكون الفعل المكون للركن المادي في هذه الصورة بفعل إذاعة أو نشر بأي وسيلة كانت أخبارا أو بيانات أو إشاعات كاذبة أو مغرضة أو أية دعاية مثيرة، بقصد تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق ضرر بالمصلحة العامة[2] .

6) جريمة الحريق والتفجير للأموال الثابتة أو المنقولة

وكذلك فإن قيام الجاني بإشعال حريقا أو أحدث انفجارا في مال ثابت أو منقول يقوم به الركن المادي لهذه الصورة من صور الإرهاب، ولا يهم بعد ذلك أن يكون المال مملوكا له أو لغيره متى كان من شأن ذلك تعريض حياة الناس أو أموالهم للخطر[3].

---

(1) راجع: الفقرات(5،6، 7، من المادة 132) من ق.ع.ي رقم 12 لسنة 1994.
(2) راجع :المادة (136) من ق.ع.ي رقم(12)لسنة 1994.
(3) راجع: المادة (137) من نفس القانون.

7) تعريض وسائل النقل والمواصلات للخطر

وفـي هذه الصـورة مـن صـور الإرهـاب يقـوم الـركن المـادي علـى فعلـي التعـريض والتعطيل، التعريض عمدا للخطر لوسيلة من وسائل النقل البريـة أو البحريـة أو الجويـة، أو التعطيل لسيرها، وكذلك التعطيل لأي وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العامة ولا يهم بعد ذلك الطريقة التي تمت بها تلك الأفعال[1].

8) حيازة المفرقعات والإتجار فيها –ع.ي- وكذلك السلاح والذخيرة –ع.ج.

كذلك فإن حيازة، أو إحراز، أو وضع، أو استيراد، أو تصنيع ،أو نقل مفرقعات أو الإتجار فيها بغير ترخيص من الجهة المختصة، أو تركيبها، من الأفعال التي يقوم عليها الركن المادي لهذه الصورة، حيث تتحقق بقيام أي فعل مما ذكر، كما تنطبق تلك الأفعال على الآلات والأدوات التي تستخدم في صنعها[2].

وأضـاف المشـرع الجزائـري السـلاح أو الـذخيرة بجانـب المفرقعـات حيـث تقـوم الجريمة بتحقق أي فعل مما ذكر إذا استهدف ذلك الفعل مفرقعات أو سلاح أو ذخيرة، واعتبر حمل السلاح أو إصلاحه أيضا إحدى جرائم الإرهاب وكل تلك الأفعال مشروطة بعدم وجود تصريح أما في حالة وجود تصريح بممارسة أي فعل مما ذكر فلا يعتبر حينئذ مجرما. [3].

9) الحرابة

يعتبر مرتكبا لجريمة الحرابة كل من تعرض للناس بالقوةسواءً في طريق عام أم صحراء أم بنيان، وسواءً أكان في البحر أم في طائرة فأخافهم وأرعبهم على نفس أو مال، أو اعترض واحدا أو جماعة لأي غرض غير مشروع [4].

10) إنشاء وتسيير أو الانخراط في الجمعيات والمنظمات والجماعات الإرهابية

وهذه الصورة نص عليها ق.ع.ج في المادة (87مكرر 3) و تضمنت عدد من الأفعال المجرمة التي إذا ما تم اقترافها فإن الركن المادي لهذه الجريمة يكون قد تحقق، وتتمثل تلك الأفعال بإنشاء، أو تسيير، أو الانخراط في الجمعيات والمنظمات

(1) راجع: المادة (138) ع.ي.
(2) راجع: المادة (144) من نفس القانون.
(3) راجع: المادة (87مكرر7) من القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات..
(4) راجع: المادة (306) من القانون رقم 12 لسنة 1994 بشأن الجرائم والعقوبات.

والجماعات الإرهابية، فيقوم الركن المادي إذا ما تحقق أحد الأفعال سواءً تم ارتكاب تلك الأفعال داخل الوطن أم خارجه، وسواء كانت تمس الجزائر أم دولة أخرى، فجميعها داخلة في نطاق التجريم الذي تضمنه النص(1).

ولم يقتصر تجريم الأفعال الإرهابية على من يقوم باقترافها سواء كان فاعلا أم شريكا، بل إن المشرع الجزائري قد مد نطاق تجريم تلك الأفعال على كل من يقوم بتمويل تلك الأفعال (2)، أو يشيد بها، أو حتى مجرد القيام بتشجيعها، لكون تلك الأفعال تساعد المجرمين على ارتكاب تلك الجرائم (3).

11) إلقاء الخطب من غير المعينين بذلك أو مخالفة الخطبة لمهمة المسجد

تضمن نص المادة:(87 مكرر10)ع.ج بعض الأفعال المتعلقة بإلقاء الخطب في المساجد أو الأمكنة العامة واعتبرها ذات صلة بالإرهاب، ومنها إلقاء تلك الخطب من غر المعينين من الجهة المختصة وغير الحاصلين على ترخيص بذلك، أو مخالفة الخطبة لمهمة المسجد إذا كان من شأنها المساس بتماسك المجتمع أو الإشادة بالأفعال المتعلقة بالإرهاب (4).

إلا أنه يلاحظ بأن الأفعال التي وردت في نص المادة (87 مكرر10) في الفقرة الأولى منه لا يتحقق بها معنى الإرهاب والذي يعني التخويف والترهيب، لكون قيام غير المكلف بإلقاء خطبة في مسجد، أو مكان عام أعد للصلاة، أو محاولة القيام بذلك ولم يكن مكلفاً به، إذا كان ذلك بحسن نية ولم تتضمن الإشادة أو التحريض على القيام بأفعال إرهابية وفقا لما تضمنه نص الفقرة (2) من ذات المادة وكانت في مجال الترغيب فهي بالتالي لا تمثل إرهابا، وكان الأولى بمثل هذا النص- الفقرة الأولى منه- أن يكون في غير موضع الأفعال التي لها علاقة بالإرهاب، بخلاف الفقرة الثانية من نص المادة نفسها(87 مرر 3) التي أوردت أفعال تدل على علاقتها بالإرهاب ومنها الإشادة بالأفعال المتعلقة بالإرهاب.

---

(1) راجع المادة(87 مكرر3) من الأمر رقم(95-11)المؤرخ في 25فبراير1995.

(2) راجع المادة (87 مكرر 4) من ق.ع.ج ،وكذلك الفقرة(ب) من المادة (3) من القانون الجزائري رقم (05-01) المؤرخ في 6 فبراير سنة 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.

(3) المادة (87مكرر4) من الأمر رقم(95-11 المؤرخ في 25 فبراير 1995، ع.ج حيث نصت على عقاب كل من يشيد بالأفعال الإرهابية أو يشجعها أو يمولها بأية وسيلة كانت.

(4) المادة (87مكرر10) من نفس القانون.

12) الإرهاب الالكتروني(Electronic terrorism).

تغيرت وتطورت وسائل وأساليب الإرهاب نتيجة للتطور التكنولوجي و المعلوماتي في مجال الاتصالات ونظم المعلومات، فظهر ما يسمى بجرائم الإرهاب الالكتروني أو الرقمي (Electronic terrorism) ، وجميعها تهدف إلى تهديد أمن وحياة المجتمع وتعريض ممتلكاته ومقدراته الاقتصادية للدمار[1] .

والأنظمة المعلوماتية والمعطيات المخزنة بها يمكن أن تكون محلا للإرهاب الالكتروني ويمكن أن تكون وسيلةً لارتكاب جرائم الإرهاب:

أ) الأنظمة المعلوماتية والمعطيات محلا لجريمة الإرهاب

تكون الأنظمة المعلوماتية محلا لجريمة الإرهاب الالكتروني عندما يتم استهداف تلك الأنظمة أو المعطيات والبرامج المخزنة بها بهدف تهديد الحياة اليومية بالخطر.

حيث يكون بإمكان مجرمي المعلوماتية شن هجوم إلكتروني على البنية التحتية للشبكة المعلوماتية بقصد تدميرها، وتوقفها عن العمل، مما يحدثآثاراً مادية واقتصادية وسياسية وثقافية خطيرة، لأن توقف الشبكة المعلوماتية يعني توقف القطاعات والمرافق الحيوية عن العمل، بالإضافة إلى توقف الحكومات الإلكترونية عن عملها، وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية [2].

ويقوم الركن المادي في هذه الصورة على أي فعل من شأنه الاعتداء على النظام المعلوماتي، أو المعطيات المخزنة بذلك النظام، ويكون من شأنه تهديد أمن وسلامة المجتمع[3]، من خلال تهديد المنشآت التي تعتمد في تسييرها بشكل كبير على المعلومات

---

(1) تشكل جرائم الإرهاب عبر الإنترنت تهديدا خطيرا للأمن والسلم سواء على مستوى مجتمع ما، أم دولة بعينها، أم على المستوى الإقليمي أو الدولي، فلقد أصبح الهكرة يقومون بعقد مؤتمرات دورية يحضرها موظفون حكوميون مثل مؤتمر (choas) في ألمانيا ومؤتمر (Defcon) في أمريكا و(Dnscon) في انجلترا، ويهدفون من وراء تلك المؤتمرات إلى تحدٍ واضح لأجهزة العدالة من أن تقوم بملاحقتهم وضبطهم جراء أعمالهم الإجرامية في مجال الجريمة المعلوماتية ومنها جريمة الإرهاب الالكتروني، راجع: عمر محمد أبو بكر يونس ، مرجع سابق، ص 650.

(2) عبد الله بن عبد العزيز بن فهد العجلان، مرجع سابق على الرابط:
http://www.f-law.net/law/showthread.php?t=28535

(3) وكأمثلة على ما تقوم به المنظمات والجماعات الإرهابية من اعتداء على أنظمة المعلوماتية بغرض تكدير وتهديد حياة الناس، ما قامت به منظمات إرهابية في عام 2000 في استراليا من تدمير أنظمة الحاسوبات التي تنظم عملية تسيير الصرف الصحي، مما تسبب في توقف الشبكة، ونتج عن ذلك حدوث أضرار صحية واقتصادية تكبدها الأهالي والمؤسسات والأجهزة الحكومية، وفي اليابان في مارس 2000 اقتحمت جماعة إرهابية تدعى جماعة (أدم كيزوكو) أنظمة أكثر من خمسين شركة من الشركات الكبرى في وعشر منظمات حكومية وعبثت ببياناتها.راجع سامي حامد عباد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، ط1، دار الفكر الجامعي، الإسكندرية،2007، ص72.

الرقمية، وعلى رأسها الكهرباء والاتصالات وشبكة الكمبيوتر[1]، فالتطور في مجال التكنولوجيا الرقمية قد جعل معظم الخدمات تسيرها أنظمة الكترونية ومن ثم فإن الاعتداء عليها بلا شك سيخلق حالة من الرعب في الوسط الاجتماعي التي تقدم له تلك الخدمات[2].

وقد أصبحت تقوم بتلك الجرائم الداخلة في الإرهاب الالكتروني دول عظمى تحت مسمى الحرب الإلكترونية[3].

ب) الأنظمة والمعطيات وسيلة لارتكاب جريمة الإرهاب

في هذه الصورة من صور الإرهاب الالكتروني يتم استخدام التكنولوجيا الرقمية في التواصل بين أشخاص ومنظمات وجمعيات الإرهاب لتسهيل مهامهم في تنفيذ عملياتهم الإرهابية، وتدريب عناصرهم في كيفية استخدام القنابل والمتفجرات وكيفية تصنيعها وجميع الأفعال التي تخدم تلك الجهات وتتسبب في تكدير الأمن والسلم العام، فغالبا ما تقوم التنظيمات والجماعات الإرهابية بأعمالها الإرهابية ضد المجتمعات الآمنة

(1) أصبح الاعتماد على شبكات المعلومات، وخصوصا في الدول المتقدمة، من الوسائل المهمة لإدارة نظم الطاقة الكهربائية، ويمكن لهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطرة وحقيقية، وخصوصا في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية، ولذلك فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي يستهدفها الإرهاب الإلكتروني، ولا يتوقف الأمر عند هذا الحد، حيث أن هنالك الكثير من الأهداف الأخرى، التي يمكن بواسطتها للهكرة المتمكنين أن يشيعوا الفوضى في الحياة المدنية، فهنالك مثلا شبكات المعلومات الطبية، والتي يمكن إذا ماتم مهاجمتها، واختراقها، ومن ثم التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى، كما أن رسالة واحدة تُنشر مثلا بالبريد الإلكتروني، مفادها أن هنالك دماء ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثارا مدمرة على الصعيد الاجتماعي.راجع: محمد محمد الألفي، مكافحة جرائم الإرهاب عبر الشبكة، موقع شبكة النباء المعلوماتية، ت.د2006/7/6،على الرابط:

http://www.annabaa.org/nbanews/55/297.htm

(2) Solange Ghernaouti –Hélie, Sécurité Informatique et réseaux, du mod, paris, 2006, P.29.

(3) يعد الإرهاب الالكتروني مجالا خصبا لأن ترتكب جرائمه من قبل دول ضد أخرى، بحيث أصبح وسيلة من وسائل الحروب التي أطلق عليها مؤخراً بالحرب الإلكترونية، والتي غالبا ما تسبق الحروب التقليدية أو تتزامن معها، وتهدف إلى شل حركة الدولة المعادية في شتى المجالات نظراً للاعتماد الأساسي في تسيير الأمور الحيوية على مجال التكنولوجيا الرقمية، وقد أدرجت ضمن جرائم الإرهاب الالكتروني نظرا لما يترتب عليها من ترويع وتخويف لإفرد المجتمع بشكل عام، ومثال ذلك ما حدث أخيراً في عام 2008 في جورجيا على يد القوات الروسية المتخصصة في مجال الحرب الإلكترونية من اعتداءات على المواقع الإلكترونية الجورجية بما فيها رئاسة الدولة ومواقع المؤسسات الهامة بما فيها المؤسسات المصرفية، كل ذلك سبق الحرب التقليدية وإطلاق النار ودخول القوات الروسية إلى الأراضي الجورجية بأسابيع.حيث بدأت المعركة الرقمية بإرسال تيار من البيانات إلى مواقع الحكومة الجورجية، وقد قدر خبراء الإنترنت في الولايات المتحدة الأمريكية في أن الهجمات الإلكترونية على البنية الأساسية للانترنت في جورجيا بدأت في 20 يوليو 2008 بضخ الملايين من الرسائل والطلبات صوب تلك المواقع بهدف الحرمان من الخدمة، ومنها التواصل عبر الإنترنت، وتعطيل المعاملات، وأفاد الخبراء بأن من ضمن المواقع التي تعرضت للاعتداء موقع الرئيس الجورجي ميخائيل ساكاشفيلي حيث تم تعطيله لأكثر من 24 ساعة، راجع الخبر على موقع مركز بحوث جرائم الحاسوب باللغة الانجليزية، قبل إطلاق النار هجمات على الإنترنت، ت.د 2008/8/13 على الربط:

http://www.crime-research.org/news/13.08.2008/3506/.

مستغلة شبكة الإنترنت لتقوية أنظمتها وتدعيمها، فضلا عن نشر أفكارها وإجراء الاتصالات اللازمة للتنسيق فيما بينها، بالإضافة إلى أنه يوجد على شبكة الإنترنت بعض المواد التي تعتبر بمثابة دروس مجانية للإرهابيين، وخاصة المبتدئين منهم، ابتداء من بيان كيفية صناعة الزجاجة الحارقة، مرورا بكيفية صنع الطرود المفخخة ،وانتهاءً بكيفية تنفيذ الهجمات[1].

فمع ظهور الإنترنت وجد الإرهاب مرتعاً خصباً، إذ أصبح أكثر ضراوةً من ذي قبل لاعتماده على التكنولوجيا المتطورة للانترنت التي ساعدت المنظمات الإرهابية في التحكم الكامل في اتصالات بعضهم ببعض[2].

ويقوم الركن المادي في هذه الجريمة على فعل التهديد، والتهديد مجرد سلوك مادي لا يتطلب تحقيق نتائج معينة لأنه من الجرائم الشكلية[3].

ويقوم التهديد الإلكتروني على أفعال من شأنها تهديد الآخرين وترويعهم كتهديد بعض الشخصيات السياسية [4]، أو الهجوم على المنشآت الحيوية[5].

وللإرهاب الالكتروني أشكال عديدة تختلف عن تلك التي ترتكب بالعالم المادي، لاختلاف النتيجة التي يحققها ذلك السلوك (التخويف والترويع والترهيب) بأسلوب رقمي قد يختلف عما يحققه السلوك المادي في الجريمة التقليدية .

وخلاصة ما سبق ومن خلال نصوص القانون اليمني والقانون الجزائري التي توضح الأفعال التي يقوم عليها الركن المادي في جريمة الإرهاب، فإنه يلاحظ على نصوص القانون اليمني أنها قد وردت متفرقة في أكثر من قسم، كما أنه تم الخلط بين الجرائم الماسة بالأمن الداخلي وتتعلق بالأسرار، والجرائم الأخرى التي يمكن أن تكون

([1]) راجع: علي محمد الانسي، مرجع سابق، ص14.

(2) Gabriel Weimann, Terror on the Internet, Potomac Books, Inc Potomac Books, Inc,2006.   http://www.taqrir.org/showarticle.cfm?id=357.

(3) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 649.

(4) وكأمثلة لتهديد الشخصيات السياسية ما حدث عام 2000 من قيام أربعة تلاميذ بريطانيين باختراق نظام البيت البيض وترك رسالة تهنئيه للرئيس بل كلينتون بمناسبة عيد السنة الميلادية، إضافة إلى التهديد بتفجير البيت الأبيض. وقيام تيمون- كندي الجنسية- في عام 1999 بإرسال رسالة إلى البيت البيض يهدد الرئيس كلينتون بالقتل، حيث تم ضبطه من قبل الشرطة الكندية بتاريخ 14 /1999/11 بعد جمله من المتابعة والتحري بواسطة الشرطة الأمريكية والكندية. راجع: سامي حامد عباد، مرجع سابق، ص71.

(5) والتهديد الذي يستهدف المنشآت الحيوية هو نوع من الترويع لأمن المجتمع، لكونه يخلق الرعب في أوساطهم، نظرا لما تمثله تلك المنشآت من أهمية على الجوانب الحياتية لهم، ومن تلك التهديدات التهديد بإطلاق فيروس يتم من خلاله قطع التيار الكهربائي عن بلجيكا بتاريخ 29 /1999/12.راجع: حامد سامي عباد، مرجع سابق، ص81.

ضمن تصنيف جرائم الإرهاب التي وردت في القانون الجزائري والقانون المصري، كما أن الجرائم الموصوفة بأفعال إرهابية في القانون اليمني هي في الأساس جرائم ذات طبيعة مادية ملموسة، يشكل الركن المادي فيها أفعال مادية ملموسة، كون المشرع اليمني حين جرم تلك الجرائم كان ينظر إليها بصفتها المادية، ولم يكن في حسبانه آنذاك التطور الذي سيطرأ على الجريمة في مجال التكنولوجيا الرقمية، بما فيها ارتكاب الجريمة عن طريق الإنترنت، لذلك فإن على المشرع اليمني وهو يدرس مشروع مكافحة الإرهاب المقدم من الحكومة أن يتنبه لذلك ويضع النصوص التي تتناسب مع تلك الجريمة في وضعها التقليدي وكذلك الرقمي، مع مراعاة أن تكون تلك النصوص نابعة من المصلحة الوطنية العليا للبلاد.

كذلك فإن القانون الجزائري مع أنه قد تضمن في نصوص قانون العقوبات تجريم الأفعال التي لها صلة بالإرهاب، إضافة إلى إصدار قانون يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب[1]، وكذلك تضمين القانون الذي صدر مؤخرا - ويتعلق بالوقاية من جرائم الإعلام والاتصال ومكافحتهما- صلاحيات واسعة في مجال الرقابة التقنية للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب[2]، إلا أن كل تلك القوانين لم تتضمن النص صراحة على تجريم الإرهاب الذي يتم عن طريق الإنترنت وتكنولوجيا المعلومات بألفاظ صريحة كما عملت بعض التشريعات الحديثة التي تم الإشارة إليها.

ويلاحظ أخيرا إمكانية تطبيق النصوص القائمة على جرائم الإرهاب الالكتروني وعلى وجه الخصوص استخدام الأنظمة المعلوماتية لارتكاب جرائم إرهابية، ففي هذه الحالة يمكن تطويع تلك النصوص للانطباق على تلك الجرائم، ومنها كافة الأفعال التي يمكن أن ترتكب من خلال الإنترنت والتكنولوجيا الرقمية، وتعد أفعال إرهابية،

---

(1) القانون الجزائري رقم (50 -01)المؤرخ في 27 ذي الحجة عام 1425 الموافق 6فبراير سنة 2005 ، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.

(2) يلاحظ من خلال نص المادة(4) من القانون رقم (09 -04) للوقاية من جرائم الإعلام والاتصال ومكافحتهما، بأن المشرع الجزائري قد خول لضباط الشرطة القضائية المنتميين للهيئة الوطنية لوقاية من جرائم الإعلام والاتصال ومكافحتهما، حق الرقابة الإلكترونية على الأفعال ذات الصلة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة، وجعل مدة الرقابة تصل إلى ستة أشهر قابلة للتجديد، بموجب إذن من النائب العام لدى مجلس قضاء الجزائر، وكذلك الرقابة في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني إلا ن هذا النص قد تضمن الرقابة كعمل وقائي للوقاية من حدوث تلك الأفعال، ولم يتضمن الإشارة إلى جرائم الإرهاب الإلكتروني، وخاصة التي تكون فيها المعطيات والأنظمة محلا لها.

فالدعايات التي تستخدمها بعض المواقع للترويج لأعمال التخريب والتفجير، وغيرها من الأعمال التي يمكن وصفها بأنها أعمال إرهابية، كذلك فإن تدريب وتعليم الإرهاب وصنع واستخدام المتفجرات، والتواصل مع قيادات ومنظمات الإرهاب لاشك أن تلك الأفعال تدخل في نطاق التجريم في كلا القانونين، ويفضل إضافة النصوص القانونية التي تجرم من خلالها الأفعال الإرهابية ذات الطبيعة التقنية التي يتم من خلالها ترويع وإرهاب الآخرين، وتشديد العقوبة على هذا النوع من الجرائم مقارنة بالإرهاب التقليدي.

ج. الركن المعنوي لجريمة الإرهاب

يقوم القصد الجنائي لجريمة الإرهاب بتوافر القصد الجنائي العام بعنصريه العلم والإرادة.

فيجب أن يعلم الجاني أنه يقوم باقتراف فعل من الأفعال المكونة لجريمة الإرهاب سواء اقتصر ذلك الفعل على الإشادة أم التمويل للأعمال الإرهابية، أم الحيازة أم الإحراز للأسلحة والذخائر والمتفجرات، أم القيام بما من شأنه المساس باستقلال الدولة وتكدير أمنها، إلى غير ذلك من الأفعال المشار إليها سابقا.

ويجب كذلك في حالة ارتكاب جريمة إرهاب إلكتروني أن يعلم الجاني بطبيعة الفعل الذي يقوم به، كأن يعلم أنه يقوم بإنشاء موقع يتم من خلاله التواصل مع الجماعات الإرهابية، أو الترويج للأفعال المكونة لجرائم الإرهاب، أو تعليم الطرق التي يتم بها تصنيع المتفجرات، وكذلك لابد أن يعلم بطبيعة الأفعال التقنية التي يقوم بها من تلاعب بالبيانات والبرامج بهدف توقيف أنظمة الخدمات الأساسية التي تدار بواسطة الأنظمة الإلكترونية، والتي أن تمت فسوف تثير الرعب والخوف في المجتمع..

كما يجب أن تتوفر الإرادة لارتكاب تلك الجرائم، فيجب أن يكون الجاني قد أقدم على ارتكاب تلك الأفعال بإرادته الحرة والمدركة لما يقوم به من أفعال.

د. العقوبات

1) في القانون اليمني

تتراوح عقوبة جرائم الإرهاب في القانون اليمني بين عقوبة الحبس لمدة لا تزيد على ثلاث سنوات في حالة إذاعة أخبار من شأنها تكدير الأمن العام، وتصل العقوبة إلى

الإعدام في حالة القيام بأفعال من شأنها الاعتداء على سلامة الجمهورية ووحدتها وسلامة أراضيها نبين منها:

- الحبس مدة لا تزيد على ثلاث سنوات لكل من أذاع أخبارا أو بيانات أو إشاعات كاذبة أو مغرضة أو أية دعاية مثيرة، وذلك بقصد تكدير الأمن العام، أو إلقاء الرعب بين الناس، أو إلحاق ضرر بالمصلحة العامة.
- الحبس مدة لا تزيد على ست سنوات لكل من حاز، أو أحرز، أو وضع، أو استورد مفرقعات، أو أتجر فيها بغير ترخيص من الجهة المختص.
- الحبس مدة لا تزيد على عشر سنوات لمن أشعل حريقا، أو أحدث انفجارا في مال ثابت أو منقول، ولو كان مملوكا له، متى كان من شأن ذلك تعريض حياة الناس، أو أموالهم للخطر، وتكون العقوبة الحبس مدة لا تقل عن ثلاث سنوات إذا حصل الحريق، أو الانفجار في مبنى مسكون، أو محل آهل بجماعة من الناس، أو في أحد المباني أو المنشئات ذات النفع العام، أو المعدة للمصالح العامة
- الحبس مدة لا تزيد على عشر سنوات لكل من عرض للخطر عمدا وسيلة من وسائل النقل البرية أو البحرية أو الجوية، أو عطل سيرها بأية طريقة، وكذلك لكل من عطل بأية طريقة وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العامة.
- الحبس مدة لا تزيد على عشر سنوات لكل من اشترك في عصابة مسلحة بقصد اغتصاب الأراضي، أو نهب الأموال المملوكة للدولة، أو لجماعة من الناس، أو لمقاومة القوة العسكرية المكلفة بمطاردة مرتكبي هذه الجرائم، وكذلك لكل من اشترك في عصابة مسلحة هاجمت جماعة من الناس، أو قاومت بالسلاح رجال السلطة العامة المكلفين بتنفيذ القوانين، و تكون العقوبة الإعدام حدا إذا نتج عن أي من أفعال الجناة المذكورة موت إنسان.
- يعاقب المحارب بالحبس مدة لا تزيد على خمس سنوات إذا اقتصر فعله على إخافة السبيل، ويعاقب بقطع يده اليمنى من الرسغ ورجله اليسرى من الكعب إذا اخذ مالا منقولا مملوكا لغيره، كما يعاقب شريكه الذي لم يأخذ مالا بالحبس مدة لا تزيد على عشر سنوات، وتكون عقوبة المحارب أو المحاربين الإعدام حدا إذا أدى فعل أي

منهم إلى موت إنسان، ويعاقب من لم يسهم في القتل بالحبس مدة لا تزيد على خمسة عشر عاما، ويعاقب بالإعدام والصلب إذا أخذ مالا وقتل شخصا، كما يعاقب من لم يسهم في الأخذ أو القتل بالحبس مدة لا تزيد على خمسة عشر عاما، وتكون عقوبة الشروع في الحرابة وقطع الطريق الحبس مدة لا تزيد على خمس سنوات [1].

2) في القانون الجزائري

تكون العقوبة في القانون الجزائري السجن من سنة إلى ثلاث سنوات وبغرامة (من 10.000 دج إلى 100.000 دج) في حالة إلقاء الخطب من غير المعينين لذلك، أو مخالفة الخطبة لمهمة المسجد، وتصل إلى السجن المؤبد في حالة إنشاء أو تنظيم أو تسيير جمعيات أو تنظيمات إرهابية، وتكون العقوبة الإعدام في حالة استهداف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها، وتوجد بين تلك العقوبات عقوبات متفاوتة بالسجن المؤقت أو الغرامة التي تصل إلى 100.000.000دج نذكر منها:

- تكون عقوبة الأفعال المنصوص عليها في المادة(87 مكرر) والتي تستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي، هي الإعدام عندما تكون العقوبة المنصوص عليها في القانون السجن المؤبد، والسجن المؤبد عندما تكون العقوبة المنصوص عليها في القانون هي السجن المؤقت من عشر (10)سنوات إلى عشرين(20)سنة، والسجن المؤقت من عشر(10)سنوات إلى عشرين(20)عندما تكون العقوبة المنصوص عليها في القانون هي السجن المؤقت من خمس (5)سنوات إلى عشر (10)سنوات، وتكون العقوبة مضاعفة بالنسبة للعقوبات الأخرى، وتطبق أحكام المادة (60 مكرر)على الجرائم المنصوص عليها في هذا القانون[2].

---

(1) راجع المواد (307،306،308) ع.ي.

(2) انظر المادة(87 مكرر1) من القانون رقم(06-23) المؤرخ في 20 ديسمبر 2006المُعَدِل والمُتَمِمْ لقانون العقوبات، وتضمنت أحكام المادة : (60) التي أشارت إليها هذه المادة - من نفس القانون ما يخص الفترة الأمنية والتي يتم تطبيقها كعقوبة تكميلية وتتضمن حرمان المحكوم عليه من تدابير التوقيف المؤقت لتطبيق العقوبة، والوضع في الو رشات الخارجية، أو البيئة المفتوحة، وإجازات الخروج، والحرية النصفية والإفراج المشروط ، كل تلك التدابير تطبق على مرتكبي الجرائم الإرهابية بموجب التعديل الأخير لقانون العقوبات 2006.

(2) المادة(87 مكرر6) من (الأمر رقم (95-11) المؤرخ في 25 فبراير 1995 .

- أي فعل لم تتضمنه النصوص الخاصة بمكافحة الإرهاب، منصوص عليه في قانون العقوبات أو أي تشريع أخر وله علاقة بالأفعال التي نصت عليها مواد الإرهاب تكون عقوبته ضعف العقوبة المنصوص عليها في القانون الذي أورد الفعل ضمن نصوصه.
- وتكون عقوبة السجن المؤبد لكل من ينشئ أو يؤسس أو ينظم أو يسير أي جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام المادة: (87)مكرر ع.ج.
- ويعاقب بالسجن المؤقت من (10)عشر إلى (20)عشرين سنة كل من انخراط أو شارك، في الجمعيات أو التنظيمات أو الجماعات أو المنظمات التي لها علاقة بالإرهاب مع معرفة غرضها وأنشطتها، وإذا ارتكبت نفس الأفعال خارج الجزائر فتكون العقوبة هي السجن من (10) سنوات إلى (20)عشرين سنة والغرامة (من 500.000الى 1.000.000 دج) حتى وإن كانت أفعالها ليست موجهة ضد الجزائر، وتشدد العقوبة بالسجن المؤبد في حال أن يكون الانخراط أو النشاط في جمعية أو منظمة أو جماعة إرهابية أو تخريبية تستهدف الإضرار بمصالح الجزائر[1].
- السجن المؤقت من خمس (5) سنوات إلى عشر(10)سنوات وبغرامة مالية (من 100.000 إلى 500.000 دج) ، لكل من يشيد بالأفعال المذكورة في المادة (87 مكرر) أو يشجعها أو يمولها بأي وسيلة كانت.

السجن المؤقت من خمس(5)سنوات إلى عشر(10)سنوات وبغرامة مالية (من 100.000 إلى 500.000 دج) لكل من يعيد عمدا طبع أو نشر الوثائق أو المطبوعات أو التسجيلات التي تشيد بالأفعال المذكورة في هذا القسم.

- يعاقب بالسجن المؤقت من عشر (10)سنوات إلى عشرين(20)سنة وبغرامة مالية (من 500.000 دج إلى 1.000.000 دج)، كل من يحوز أسلحة ممنوعة أو ذخائر أو يستولي عليها أو يحملها أو يتاجر فيها أو يستوردها أو يصنعها أو يصلحها أو يستعملها دون رخصة من السلطة المختصة، ويعاقب بالإعدام مرتكب الأفعال

(1) المادة (87 مكرر6) من (الأمر رقم (95-11) المؤرخ في 25 فبراير 1995.

المنصوص عليها في الفقرة السابقة عندما تتعلق هذه الأخيرة بمواد متفجرة أو أية مادة تدخل في تركيبها أو صناعتها.

- يعاقب بالسجن المؤقت من خمس(5) سنوات إلى عشر(10)سنوات وبغرامة مالية (من 100.000 دج إلى 500.000 دج)، كل من يبيع عن علم أسلحة بيضاء أو يشتريها أو يوزعها أو يستوردها لأغراض مخالفة للقانون.

- الحبس من سنة (1)إلى ثلاث(3)سنوات وبغرامة (من 10.000 دج إلى 100.000 دج) لكل من أدى خطبة أو حاول تأديتها داخل مسجد أو في أي مكان عمومي تقام فيه الصلاة دون أن يكون معيناً أو معتمدا من طرف السلطة العمومية المؤهلة ومرخصا له من طرفها للقيام بذلك، ويعاقب بالحبس من ثلاث (3)سنوات إلى خمس(5) سنوات وبغرامة (من 50.000 دج إلى 200.000دج) كل من أقدم، بواسطة الخطب أو بأي فعل، على أعمال مخالفة للمهمة النبيلة للمسجد أو يكون من شأنها المساس بتماسك المجتمع أو الإشادة بالأفعال المشار إليها في هذا القسم[1].

---

(1) المادة (87مكرر10) من الأمر رقم (95-11 المؤرخ في 25 فبراير 1995)المُعَدِل والمُتَمِمْ لقانون العقوبات.

المبحث الثاني

جرائم الاعتداء على الأموال في نطاق المعلوماتية

(information at treasury aggressor crimes)

إذا كانت الجرائم المادية التي تقع على الأموال من سرقه ونصب وخيانة أمانة وغيرها تحدث عن طريق أفعال مادية ملموسة، وتفضي إلى الخسائر المادية، فإنه باتساع وانتشار التقنية الحديثة أصبحت الجرائم التي ترتكب في مجال المعلوماتية لا تتطلب القيام بأفعال مادية لاقترافها، بقدر ما تتطلب المجهود الذهني، ومع ذلك فهي أكثر خطورة [(1)]، حيث أضحت أغلب تلك الجرائم ترتكب بواسطة النظم المعلوماتية، ومنها جرائم الاعتداء على المعلومات المدرجة في نظام المعالجة الآلية للبيانات، وذلك ما دفع العديد من الدول إلى تعديل قوانينها أو إصدار قوانين تتناسب مع هذا النوع الجديد من الإجرام.

وسنقتصر على تناول جريمتي السرقة والنصب، في مجال المعلوماتية، حيث سيتم إيضاح كل جريمة في مجال المعلوماتية مقارنة بالقواعد العامة لبيان مدى كفاية القوانين التقليدية في مواجهتها وفيما إذ كانت الضرورة تستدعي مواجهتها، من خلال نصوص حديثة، تتناسب مع حداثة الجريمة وارتباطها بالجانب التقني، أسوة بالدول السباقة في هذا المجال.

ونظرا لكون المشرع اليمني لم يقم بسن قانونا يتضمن الحماية الجنائية للمعلوماتية بشكل عام، بما فيها جرائم الاعتداء على الأموال في نطاق المعلوماتية، أو حتى نصوص قانونية تضاف إلى قانون العقوبات، وتعاقب من يقوم باقتراف أي من الجرائم ذات الصلة بالمعلوماتية، فسوف يتم الاقتصار على نصوص قانون العقوبات التقليدية لبيان ما إذا كانت تلك النصوص تفي لمواجهة تلك الجريمة.

---

(1) ومن تلك المخاطر(سرقة المعلومات الحساسة بشتى أنواعها العسكرية والمالية والاقتصادية والسياسية، وزرع الفيروسات التي تدمر قواعد البيانات وتدمر أجهزة الكمبيوتر وتقوم بالتلصص على الأسرار الشخصية، والتحرش والابتزاز ونشر المواد الإباحية، إذ يقدر الخبراء حجم الخسائر التي تكبدتها البنوك العربية خلال العامين الماضيين بسبب الاختراقات التي تعرضت لها الشبكات بحوالي 200 مليون دولار، وقد تم الكشف عن هذه الأرقام خلال مؤتمر العمل المصرفي الإلكتروني والأمن الإلكتروني، الذي أقيم في دبي لمدة يومين. لمزيد من الإيضاح راجع: أمين عباس، الجريمة الإلكترونية والقانون في اليمن، موقع وكالة الأنباء اليمنية سبا، ت.د 2009/3/19، على الرابط:
http://www.sabanews.net/ar/news142248.htm

المطلب الأول

جريمة السرقة في مجال المعلوماتية (information theft crime)

تعرف جريمة السرقة بأنها: (اختلاس مال منقول مملوك للغير بنية التملك)(1).

وتعرف في القانون اليمني بأنها: (اخذ مال منقول مملوك للغير خفية مما يصح تملكه على نصاب من المال في غير شبهة، ومن حرز مثله بقصد تملكه دون رضاء صاحبه وكان المال المسروق تحت يد صحيحة)(2).

كما تعرف في القانون الجزائري بأنها (كل من اختلس شيئا غير مملوك له يعد سارقا)(3)، و يلاحظ على هذا التعريف بأنه قد أاقتصر على تعريف مرتكب الجريمة وليس الجريمة، إلا أنه قد تضمن أركان جريمة السرقة من خلال سياق وعبارات النص.

ومن خلال ما تقدم يتضح بأن جريمة السرقة تقوم على محل يتمثل بمال منقول مملوك للغير، و ركن مادي يتمثل في فعل الاختلاس لنقل ذلك المال إلى حيازة المتهم بدون رضا صاحبه، و ركن معنوي يتمثل بنية التملك للمال المختلس، وذلك ما سيتم التطرق إليه لإيضاح مدى تحقق تلك الأركان في جريمة السرقة المنصبة على المعلوماتية.

أولا: العوامل المكونة لجريمة السرقة

يشترط لتحقق جريمة السرقة أن يكون محلها مالا، ويشترط في ذلك المال أن يكون منقولا، و له قيمة، وأن يكون مملوكا للغير(4). وبالتالي فلا تقع الجريمة إذا تخلف شرط من الشروط المذكورة وفقا للقواعد العامة. فهل تعد المعلوماتية مالا ؟ وما طبيعة ذلك المال؟ وهل تعتبر في عداد المنقولات و قابلة للتملك، مثلها مثل الأموال المادية ؟ ذلك ما سيتم الإجابة عنه تباعا.

(1) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سايق، ص226.
(2) المادة (294) من قانون الجرائم والعقوبات اليمني رقم(12) لسنة1994.
(3)المادة(350) من الأمر رقم (56- 156) يتضمن قانون العقوبات المعدل والمتمم.
(4) راجع المادة (294)من قانون الجرائم والعقوبات اليمني رقم 12 لسنة 1994، و المادة (350)من قانون العقوبات الجزائري، وبمقارنة القانون اليمني بالجزائري نجد أن القانون اليمني قد اعتبر محل جريمة السرقة هي المال المادي، واشترط أن يكون ذلك المال منقولا ومملوكا للغير، وأضاف شرطا آخر لم يتضمنه القانون الجزائري، وهو أن يبلغ ذلك المال نصابا محددا حتى تقام العقوبة الحدية، ويتمثل النصاب بما يعادل قيمة نصف جنيه ذهب أبو ولد، والقانون الجزائري من ضمن عدد من القوانين التي تعبر عن المحل المادي لجريمة السرقة بأنه شيء مملوك للغير أو يخصه، ومن تلك القوانين كذلك الفرنسي والألماني والبلجيكي والسويسري والنمساوي فتلك القوانين تعبر عن لفظ المال بلفظ الشيء. لمزيد من التفصيل حول القوانين التي تعتبر المحل المادي للسرقة بالشيء. راجع: هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص129 .

1- طبيعة المال

يقصد بالمال وفق القانون المدني (كل شيء يتمول به، ويمكن الاحتفاظ به لوقت الحاجة، إذا كان التعامل به مباحا شرعا، وكان غير خارج عن التعامل بطبيعته)(1) .

و الأموال ليست جميعها صالحة لأن تكون محلا للسرقة، بحيث يمكن التفرقة بين نوعين من الأموال : أموال تدخل في دائرة التعامل، ومن ثم تصلح لأن تكون محلا للسرقة وأموال لا تدخل في دائرة التعامل، ولا تكون صالحة للتملك ومن ثم لا تقع عليها جريمة السرقة.

وتنقسم الطائفة الثانية من الأموال إلى قسمين، القسم الأول: أموال خارجة عن التعامل بطبيعتها، مثل الماء في البحار، والسمك في الماء، والقسم الثاني: الأموال التي تخرج عن دائرة التعامل بحكم القانون.

ويشترط في الشيء محل السرقة أن يكون ماديا، فالشيء المادي هو الذي يصلح محلا للسرقة، وهو المال الذي يمكن الاستئثار به والاستيلاء عليه وحيازته، بغض النظر عن الصورة التي تكون عليها مادة الشيء، فقد أظهر التقدم أشياء وإن كانت غير منظورة إلا أنها ملموسة، ولها كيان مادي، بحيث يمكن حيازتها والسيطرة عليها.

ويجب أن يكون الشيء المسروق ذا قيمة، فإذ انتفت عنه القيمة فلا يصلح أن يكون موضوعا للسرقة، إلا انه لا يشترط في المال أن يكون ذا قيمة معينه فضآلة القيمة أو كثرتها لا أثر لها على قيام الجريمة، إلا أن المشرع اليمني قد حدد نصابا للمال محل السرقة الحدية وهو نصف جنيه ذهب أبو ولد (2)، وعليه فلا يعاقب المتهم بجريمة السرقة الحدية إذا كان المسروق اقل من النصاب المحدد.

وبهذا الخصوص يجب التفرقة بين نوعين من المال:

الأول: المال المعلوماتي المادي

الثاني: المال المعلوماتي المنطقي

فأما النوع الأول من المال المنقول ماديا فإنه لا تثار شبهة أو خلاف حول وقوع سرقته، تحت طائلة العقاب، وفقا لنصوص قانون العقوبات اليمني والجزائري، وكافة

---

(1) المادة (112) من القانون المدني اليمني رقم (14)لسنة 2002.

(2) المادة (294) من قانون العقوبات رقم (12) لسنة 1994.

القوانين التقليدية، فسرقة مكونات الحاسوب المادية من جهاز وطابعة وغيرها من مكونات الحاسوب المادية لا تثير أدنى شبهة في تطبيق النصوص التقليدية عليها.

كما أن الاستيلاء على البيانات المخزنة إلكترونيا بسرقة أوعيتها أو وسائطها المادية، كالا شرطة والأقراص المغناطيسية تقع تحت طائلة العقاب حسب رأى البعض[1] وبالتالي ففي حالة الأخذ بهذا الرأي فإن من يقوم بالاستيلاء على البيانات عن طريق اختلاس أوعيتها يعد مقترفا لجريمة سرقه، ويعاقب وفقا للنصوص التقليدية في قوانين العقوبات .

أما الأموال المعلوماتية المنطقية فهي التي تثير إشكالا حول تطبيق نصوص القوانين التقليدية عليها، حيث أثار اختلاسها جدلا فقهيا كبيرا حول مدى انطباق معنى الاختلاس عليها[2].

ويقصد بالمال المعلوماتي المعنوي: (مكونات العناصر المنطقية للنظام المعلوماتي من برامج وبيانات صالحه للاستخدام أي المعالجة الآلية) [3].

ولبيان مدى خضوع المعلومات والبرامج التي تم معالجتها آليا للنصوص التقليدية في جريمة السرقة إذا انصبت السرقة على محتوى النظام المعلوماتي، فلا بد من إيضاح رأي الفقه بهذه المسألة، حيث انقسم الفقه مابين رأي معارض لاعتبار المعلوماتية مالا، ومن ثم عدم خضوعها للقواعد العامة في جريمة السرقة، ورأي يعتبر المعلوماتية مالا، ومن ثم فإنها تخضع للقواعد العامة في جريمة السرقة، وثالث يعتبر المعلوماتية مجموعة مستحدثة من القيم، وسيتم إيضاح ذلك تباعا:

أ- المعلومات حرة المرور

يستند الرأي القائل بأن المعلوماتية ليست مالا، وهي حرة المرور إلى:

1) أن مكونات الجانب غير المادي من النظام الآلي لمعالجة المعلومات لايتحقق فيها وصف المال وفقا للمعنى المتداول، وإن كانت قابلة للاستغلال المالي، فالبرنامج هو

---

(1)أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، رسالة دكتوراه في القانون الجنائي دراسة مقارنه، دار النهضة العربية القاهرة، 2000، ص452، وص462، وص482.

(2) محمد عبد الظاهر حسين، المسئولية القانونية في مجال شبكة الإنترنت، المؤسسة الفنية للطباعة والنشر، 2004،ص53.

(3) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005 ،ص291.

إبداع فكري قابل للاستغلال المالي، ومن ثم يطبق بشأنه قانون حماية حق المؤلف(1)، وليس قانون السرقة، أما المعلومة فتعني تسجيل لواقع قائم كحالة أو رقم أوصفه، وقد تكون سرية والاعتداء عليها يمثل انتهاكا لسريتها وليس سرقة لها، وقد تكون غير سرية وفي هذه الحالة فإن الإطلاع عليها مباح للكافة، ولا جريمة عندما تكون مجانية، أما عندما تكون بمقابل فإن الحصول عليها دون دفع المقابل يمثل سرقة للمنفعة أو الفائدة المرجوة من هذه المعلومة (2).

2) لا يمكن اعتبار المعلوماتية مالا، قياسا على التيار الكهربائي، لأن المعلومة الواحدة يمكن تسجيلها على أكثر من وسيط مادي مختلف، بحيث يوجد عدد لاحصر له من المعلومات الواحدة، وهو ما يختلف تماما بالنسبة للكهرباء، كما أنه لا يمكن احتساب المقدار الذي تم اختلاسه على وجه الدقة بالنسبة للمعلومات، بخلاف الكهرباء(3).

ويساند هذا الرأي رأي آخر يرى أن المعلوماتية لا تصلح أن تكون مالا أو محلا للسرقة، إلا إذا اقترنت بالمادية، فلا تصلح البرامج المعلوماتية التي يتم الاعتداء عليها محلا لجريمة السرقة، مهما ترتب عليها من خسائر إلا في حالة وجودها مسجله على دعامات أو اسطوانات (4).

([1]) تضمنت المادة (4) من الأمر الجزائري رقم 05/03 المؤرخ في 2003/7/19 المتعلق بحق المؤلف والحقوق المجاورة، برامج الحاسب الآلي وقواعد البيانات ضمن الحقوق المحمية للمؤلف، راجع محي الدين عكاشة، حقوق المؤلف على ضوء القانون الجزائري الجديد،ط2،ديوان المطبوعات الجامعية ،الجزائر،2007،ص83.
وراجع ايضا:
Bouder Hadjira, Quelle protection pour les programmes d'ordinateur en droit Algérien? Revue algérienne des sciences juridiques économiques et politiquesfacilté de droit de ben aknoun-Alger,volume'&n°02/2004,p94 et après
أما القانون اليمني رقم (19)لسنة 1994 بشأن الحق الفكري فلم يتضمن نصا قانونيا يجرم الاعتداء على برامج الحاسب الآلي وقواعد البيانات، ومع ذلك فيوجد من يرى بإمكانية تطبيق نصوصه عليهما، لأن المصنفات المحمية التي أشارت إليها المادة(3) من القانون قد وردت على سبيل المثال لا الحصر حيث أن المادة المذكورة بعد أن أوردت قائمة بالمصنفات المحمية اختتمتها بعبارة" وبوجه عام كل عمل يكون التعبير فيه بالكتابة أو الصوت أو الرسم أو التصوير أو التجسيم أو الحركة أو غير ذلك"، فإن حماية قانون الحق الفكري تشمل ما لم يرد ذكره في تلك المصنفات إذا توفر فيها شرط الإبداع. راجع: محمد أحمد المخلافي، العولمة والملكية الفكرية، ط1، مؤسسة العفيف الثقافية، صنعاء، اليمن، 2002، ص83.

(2) عمر الفاروق الحسيني : جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون- جامعة الإمارات العربية المتحدة،2000،ج 1، ص332. وعفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط2، بدون ذكر دار وبلد النشر، ص241. و أحمد خليفة الملط ، مرجع سابق، ص294.

(3) نائلة عادل محمد فريد قورة، جرائم الحاسوب الآلي الاقتصادية، رسالة دكتوراه، كلية الحقوق –جامعة حلوان، ط1، 2005م، منشورات الحلبي الحقوقية، بيروت، ص162.

(4) احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص453، وص462، وص481.

ب- المعلوماتية مالا

بينما يستند أصحاب الرأي القائل بأن المعلوماتية تعد مالا مثل سائر الأموال إلى:

1) قابلية المعلوماتية للحيازة والاستئثار، إضافة إلى أنها تمثل قيمة اقتصادية فهي تطرح في السوق للتداول، مثل أي سلعة أخرى، ولها سوق تجارية تخضع لقوانين السوق، كما أنها منتج، بصرف النظر عن دعامتها المادية وعن عامل قدمها، ولها علاقة بمالكها مثل علاقة المالك بالشيء الذي يملكه [1].

2) إذا كان الفقه التقليدي لا يعترف للمعلومات بصفة المال، فإن الفقه الحديث يخالف ذلك على أساس أن معيار الشيء لا يعتمد على ماله من كيان مادي، وإنما على أساس قيمته ألاقتصادية، وأن القانون الذي يرفض إسباغ صفة المال على شيء له قيمة اقتصاديه سيبقى حتما على خلاف الحقيقة [2].

3) أن التسليم بأن المال المعلوماتي المعنوي غير قابل للاستحوانوليس مالاً ، وبالتالي فهو غير قابل للسرقة، سيؤدي حتما إلى تجريده من الحماية القانونية الجنائية ويفتح المجال أمام قراصنة البرامج والمعلومات لارتكاب جرائمهم [3].

4) يمكن قياس المال المعلوماتي على الطاقة الكهربائية، واعتباره مالا يخضع للقواعد العامة للسرقة، بالرغم من أنه ليس ذا طبيعة مادية، فمبدأ تجريم الاستيلاء على الطاقة يطبق على كل قوة أو طاقة يمكن إخضاعها لسيطرة الإنسان، ويكون بوسعه أن يوجهها على النحو الذي يحقق منفعته، وعليه فإن المعلومات والأفكار تعتبر طاقة ذهنية [4]، وقد اخذ بفكرة قياس سرقة المعلومات أو البرامج على سرقة التيار الكهربائي البعض[5]، مع خلاف في المعيار، حيث يتمثل المعيار وفقا لهذا الرأي بالإضرار بالغير، ويتحقق ذلك بالنسبة لسرقة التيار الكهربائي وكذلك سرقة المعلومات وبرامج الحاسب الآلي.

---

(1) وهذا الرأي للأستاذ (Catla) مشار إليه لدى عبدا لله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط3، دار النهضة العربية، القاهرة،2004، ص168.

(2) راجع عبدا لله حسين محمود، مرجع سابق، ص169، وهو رأي الأستاذ (Carbonnier).

(3) هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية القاهرة، 1992، ص52.

(4) آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط1، دار هومة للطباعة والنشر، الجزائر،2006 ،ص29.

(5) خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية المصري، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص177.

ج- **المعلوماتية مجموعة مستحدثة من القيم**

يستند أصحاب الرأي القائل بأن المعلوماتية مجموعة مستحدثة من القيم إلى [1]:

1) أن المعلومة -استقلالا عن دعامتها المادية- تعد قيمة قابلة للاستحوانوتقوً م وفقا لسعر السوق، متى كانت غير محظورة تجاريا، بغض النظر عن دعامتها أو قدمها[2].

2) أن المعلومة بوصفها قيمة فإنها تندرج في إحدى القيمتين، إما قيمة معنوية ذات طابع اقتصادي، وبالتالي تكون جديرة بالحماية، وإما قيمة مادية فتصبح محلا للحق، فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية، وحيث إن للمعلوماتية قيمة فإنها تصلح لأن تكون محلا للسرقة [3].

2- طبيعة المنقول

إضافة إلى أنه يتطلب في محل جريمة السرقة أن يكون مالا فإنه يشترط في ذلك المال أن يكون منقولا(movable).

والمنقول هو كل ما يمكن نقله من مكان إلى آخر بفعل الجاني[4]. ومفهوم المنقول في القانون الجنائي أوسع من مفهومه في القانون المدني، فما يعتبر عقاراً في القانون المدني قد يعتبر منقولاً في القانون الجنائي، مثل العقار بالتخصيص في حالة فصله وسرقته [5].

وبداهة وبمقتضى أن يكون محل الاختلاس قابلا للنقل من مكان إلى آخر، فيتعين أن يكون المنقول ذا طبيعة مادية، وبالتالي فلا تصلح الأموال المعنوية لأن تكون محلا للسرقة، لانتفاء صفة المنقول عنها، فالأفكار والحقوق الشخصية والعينية والمنافع لاتصلح لأن تكون محلا للسرقة إلا إذا اتخذت تلك الحقوق مظهرا ماديا يتمثل في كتاب

(1) وهم بعض فقهاء الفقه الحديث في فرنسا (Vivant, Catala) حيث وردت أرائهم في مؤلف عبد الله حسين علي محمود، مرجع سابق، ص168، وكذلك في مؤلف أحمد خليفة الملط، مرجع سابق، ص295، وص296 .

(2) عبد الله حسين علي محمود، مرجع سابق، ص168.

(3) أحمد خليفة الملط،، مرجع سابق، ص295، وص296 .

(4) حسني الجندي، مجدي عقلان، شرح قانون العقوبات اليمني، دار إقراء للنشر والتوزيع، بدون تاريخ طبعة، ص10 . وقد اشترط القانون اليمني في المال المسروق أن يكون منقولا بنص المادة (294) من قانون العقوبات اليمني التي عرفت السرقة بأنها اخذ مال منقول مملوك للغير، فالسرقة لا تقع على العقارات لعدم قابليتها للنقل من مكانها ويعتبر منقولا كل ما يمكن نقله من مكان إلى أخر وبذلك تعتبر منقولات العقارات بالتخصيص والعقارات بالاتصال متى انفصلت، ولا يهم بعد ذلك شكل ونوع وطبيعة المال فيدخل في ذلك الماء والكهرباء والغاز .

(5)عبد الله حسين محمود، مرجع سابق، ص 166، وراجع عمر الفاروق الحسيني، مرجع سابق، ص333.

أو وثيقة أو محرر فإنها تكون منقولات قابلة للاختلاس، ومن ثم تقع عليها جريمة السرقة [1]. كما يشترط أن يكون للمنقول قيمة فإذا لم تكن له قيمة على الإطلاق فلا تتحقق جريمة السرقة.

ويمكن القول بأن الاستيلاء على البيانات المخزنة إلكترونيا باختلاس وسائطها المادية كالبطاقات المثقبة أو الأشرطة أو الأقراص الممغنطة، كل ذلك لا يثير شبهة في وقوع تلك الأفعال تحت طائلة العقاب، وفقا لنصوص قوانين العقوبات التقليدية المتعلقة بالسرقة، لكون هذه الأوعية لها قيمة مادية ملموسة، فهي بمثابة منقولات مادية، ولا يوجد خلاف بين الفقهاء حول سرقة كيانها المادي، وكذلك البرامج والمعلومات التي تم معالجتها آليا وتم تحويلها إلى اسطوانات أو كيانات مادية أخرى [2].

وتثار الإشكالية حول سرقة المعلوماتية بذاتها أي مستقلة عن الكيانات المادية التي يمكن تخزينها بواسطتها، فهل تعد المعلوماتية منقولات يمكن إخضاعها لعقوبة جريمة السرقة في حال الاستيلاء عليها ؟

وبهذا الخصوص انقسم الفقه إلى اتجاهين:

أ- المعلوماتية ليست منقولا

1) أن المعلومات المخزنة بالنظام المعلوماتي أو بأي وسيط آخر لا تعتبر في حد ذاتها أشياء مادية، فلا يتصور انتزاعها أو حيازتها كما في المنقول، وبالتالي يستبعد أن تكون محلا للسرقة، إلا أن المستندات المثبتة للمعلومات أو التي تكون وسيلة للتسجيل عليها هي التي تصلح للسرقة، لأن لها كياناً مادياً [3].فتجوز السرقة للسند المثبت للحق، كالسند المثبت للدين، أو للمخطوط الذي سجل فيه المؤلف أفكاره، أو اللوحة المرسومة.

2) أن الأشياء التي تظهر على شاشة النظام المعلوماتي وإن كانت تبدو كنتاج لنشاط إنساني، ويمكن تقديرها بالجهد الفني الذي يبذل في إعدادها، إلا أنها لا تعتبر بمثابة شيء، ولا تعتبر مكتوبة بالمرة، وبالتالي لا تصلح أن تكون محلا للسرقة، كما أن الموجات التي تنقل بها المعلومات هي من طبيعة غير مادية، إضافة إلا أنها متاحة

---

(1) هشام فريد محمد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص228.
(2) هشام فريد محمد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع السابق، ص230.
(3) راجع أحمد خليفة الملط، مرجع سابق، ص299.

للجميع ولا يمتلكها أحد وبالتالي فلا يمكن أن تكون محلا للسرقة حسب هذا الرأي[1].

3) أن المعلومات لا تعتبر من قبل الأشياء، والسرقة لاترد إلا على أشياء، وقد يتم الحصول عليها بالسمع، أو بالاطلاع عليها من الشاشة، أو بإعادة نسخ البرامج على دعامات يملكها الجاني ذاته[2].

4) تفترض في جريمة السرقة انتقال الشئ محل فعل الاختلاس من حيازة المالك إلى حيازة من أختلسه، ولا يتصور ذلك بالنسبة للمعلومات، لأنها تبقى لدى المالك ولا يمكن تجريده منها، حتى في حالة القيام بنسخها وحذف النسخة التي لدى المالك لوجود برامج تجعل المالك يتمكن من استعادتها، كما أن حذف البيانات قد يشكل جريمة أخرى [3].

ب- تكييف المعلوماتية بالمنقول

1) أن المعلومة يمكن أن تنقل عن طريق الشخص الذي قام بالتقاطها بالسمع أو المشاهدة وتدوينها أو تسجيلها على دعامة ومن ثم عرضها للبيع، وبالتالي فإن المعلومة في هذه الحالة تنقل من ذمة شخص إلى ذمة آخر[4].

2) تفسير بعض الفقهاء لكلمة شيء - وردت في بعض القوانين منها القانون الفرنسي والجزائري – تفسيرا واسعا بحيث تشمل الأشياء المادية وغير المادية وهو ما يجعل المعلومات تدخل في نطاق هذه الكلمة [5].

3) أن سرقة المعلومات المستقلة عن الدعامات هي السبب الذي من أجله أدانت محكمة النقض الفرنسية في قضية (Logabax) العامل الذي قام بنسخ مستندات سرية بدون علم ورضا صاحب المشروع، كذلك إقرار محكمة النقض الفرنسية في قضية(Bourquin) صراحة بأن المعطيات المعلوماتية أشياء قابلة للسرقة ، حيث أيدت المحكمة إدانة عاملين بورشة التأليف الضوئي بمطبعة (Bourquin)

---

(1) جميل عبد الباقي الصغير، المواجهة الجنائية لقرصنة البرامج التلفزيونية المدفوعة الأجر، دار النهضة العربية، القاهرة، 2002، ص24وص25.
(2) أحمد خليفة الملط، مرجع سابق، ص299.
(3) نائلة عادل محمد فريد قورة ، مرجع سابق، 160.
(4) أحمد خليفة الملط، مرجع سابق، ص300.
(5) ورد هذا الرأي – رأي في الفقه الفرنسي - في مؤلف نائلة عادل محمد فريد قورة، مرجع سابق ص 158.

بجريمة السرقة لقيامهما داخل المطبعة وباستخدام معالجاتهما، وبهدف تأسيس مشروع منافس بنسخ 47 اسطوانة معلوماتية تحوي معلومات للعملاء على جانب كبير من الأهمية والقيمة التجارية، بالإضافة إلى الاستيلاء على 70 اسطوانة مسجلاً عليها كل عمليات التأليف الضوئي التي باشرتها المطبعة، وفي حكمها ذكرت المحكمة العليا أن قضاة الموضوع قد أثبتوا سائر العناصر التكوينية للجريمة في حق المتهمين، وأن الأخيرين قد أدينا بجريمة سرقة 70اسطوانه ممغنطة من جهة وسرقة المحتوى الإعلامي لـ47 اسطوانة ممغنطة من جهة ثانية خلال المدة اللازمة لنسخ وإعادة إنتاج المعلومات إضرار بالمطبعة المالكة لها، حيث يعد هذا الحكم على جانب كبير من الأهمية، فمن ناحية يأتي أكثر وضوحا في تحديد المحل الذي تنصب علية جريمة السرقة، ألا وهي المعلومات في ذاتها، ومن ناحية أخرى فهو يتعرض لنسخ المعلومات المسجلة على الأقراص الممغنطة بصفة خاصة [1] وقد خالف هذا الرأي بعض الفقهاء في الجزائر واعتبروا بأن السرقة في هذه الحالات هي سرقة مؤقتة للشريط المحتوي على المعلومات وفقا لقرارات غرفة النقض الفرنسية[2].

3- ملكية الغير للمال

يلزم في المحل الذي تقع عليه جريمة السرقة علاوة على كونه مالا منقولا أن يكون ذلك المال المنقول مملوكا للغير، ويترتب على ذلك خروج المال المملوك للجاني من محل الجريمة، فلا يعد سارقا من يقوم بأخذ ماله حتى لو كان معتقدا ملكيته للغير،

(1) مشار إليه لدى هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص244، ص246، و كذلك لدى نائلة عادل محمد فريد قورة، مرجع سابق، ص126، وص131،

(2) الأستاذة نصرون وردية، حيث اعتبرت خطا البعض بتفسير حكم محكمة النقض الفرنسية في قضية (Logabax) بسرقة المعلومات مستقلة عن الدعامات، و كذلك إقرار محكمة النقض الفرنسية في قضية (Bourquin) بأن المعطيات المعلوماتية أشياء قابلة للسرقة، وقد يكون ذلك بسبب الترجمة الخاطئة، وبالتالي فقد استبعدت السرقة في قرار الغرفة الجنائية بمحكمة النقض الفرنسية المؤرخ في 1979/1/8 في قضية لوقبكس، وكذلك في قضية بوركان بالقرار المؤرخ في 1989/1/12، وكذلك في قضية انطونيولي في 1989/3/1، وتتمثل هذه القرارات في العامل الذي اقرض(سلف) أشرطة من رب العمل لاستنساخ محتواها(قائمة الزبائن) واستعمل وثائق رب العمل للقيام ببطاقات المعلومات لفائدة منافس هذا الأخير، وكيفت الغرفة الجنائية هذه الواقعة بالسرقة المؤقتة لحامل المعلومات(أي خروج الأشرطة من المؤسسة لإعادة إنتاج المعلومات) فالسرقة في جميع الأحوال لم ترد على المعلومات في ذاتها، وإنما سرقة مؤقتة للشريط المحتوي على المعلومات.

ومثال ذلك اعتقاد الشخص بان المال الذي قام بحيازته مملوك للغير، مع أنه قد انتقل إليه بالميراث[1].

كما أن جريمة السرقة لا تتحقق في حالة انتزاع الشخص مالا مملوكا له من حيازة غيره، حتى لو كان الغير أولى بالحيازة كما لو كان الحائز مستأجرا أو مستعيرا.

و لا يعد سارقا من يأخذ أموالا مباحة مثل الطير في السماء والسمك في الماء، بعكس ما إذا أصبحت الأموال المباحة في يد مالك لها، أي من قام بالاستيلاء عليها، وأصبحت ضمن ممتلكاته فإن الاعتداء عليها وأخذها يعد جريمة سرقة، إذا تحققت باقي الأركان، وعلى العكس من ذلك تعتبر الجريمة قائمة بحق من يجد مالا مفقودا، وينوي أخذه والتصرف فيه تصرف المالك وذلك لكون المال المفقود يظل مملوكا لصاحبه طالما لم يتنازل عنه أو يتصرف فيه[2].

وبخصوص مدي انطباق شرط ملكية الغير للمعلوماتية أو المال المعلوماتي فقد تباينت آراء الفقهاء بذلك:

أ- المال المعلوماتي مملوكا للغير

1) لأن البرامج محمية بحق المؤلف والبرنامج ملكا لمن يبتكره، وتكون القضية في تحديد صاحب الحق على البرنامج أو المعلومات [3].
2) إن جوهر الاختلاس هو دخول الشيء في حيازة الجاني وهو الشرط المفترض لوقوع السرقة على شيء منقول مملوك للغير، مثل المعلومات، باعتبارها ذات قيمة اقتصادية وسياسية، وأن سبب وجود المعلومات ليس قابليتها للنقل فقط، بل إن المعلومات المنسوخة على دعامات والمعالجة آليا تعترف بحقوق الملكية لمن قام بعمل المعالجة الآلية لها، كما أن سرقة الدعامات المملوكة للغير والمنسوخ عليها معلومات هو سرقة للمعلومات ذاتها، لأن الدعامات بدون معلومات لا قيمة لها، وبالتالي ففي حالة السرقة ينتقل المال المعلوماتي من حيازة مالكه إلى حيازة الغير[4].

---

(1) عبدا لله حسين علي محمود، مرجع سابق، ص282.
(2) لمزيد من التفصيل حول ملكية المال للغير راجع: حسني الجندي، شرح قانون العقوبات اليمني، دار إقراء للنشر والتوزيع، بدون تاريخ طبعة، ص116 وما بعدها.
(3) عبد المهيمن فكري، القسم الخاص في قانون العقوبات المصري، ط7، دار النهضة العربية، القاهرة، 1997، ص771 ، مشار إليه لدى أحمد خليفة الملط، مرجع سابق، ص304 .
(4) وهذا الرأي مشار إليه لدى حمد خليفة الملط، مرجع سابق ، ص304

3) أن الاستيلاء على المعلومات المنسوخة على دعامات هي سرقة للمعلوماتية ذاتها وإن كانت محمية بقواعد الملكية الفكرية، وينتج عن ذلك قبول السرقة حماية لمبدعيها وأصحاب المؤسسات المنتجة للبرامج. فإذا كان المال المعلوماتي مملوكا للغير فقد تحققت جريمة السرقة، سواء أكان صاحب المال معروفا أم غير معروف[1].

4) رأي في الفقه العربي يؤكد بأن البرامج والبيانات المعالجة آليا تصلح لأن تكون محلا للملكية، باعتبار أن التحليل المنطقي الذي لا يمكن إنكاره هو ملكيتها لشخص ما، وبالتالي فهي ليست ملكا للسارق[2].

ب-المعلومات ليست ملكاً لأحد

ذهب رأي أخر إلى أن المعلوماتية لاتنطبق عليها شروط ملكية المال للغير مثل الأموال المادية لأسباب منها:

1) لأن المعلومات كالأفكار لا يمكن نسبة ملكيتها إلى شخص محدد، كما يصعب الاستئثار بها، فالمعلومات ليست موضوعا لحق الملكية، ففي مجال الإبداع غير المادي، لا يتصور الحصول على هذا الإبداع إلا نادرا، وفي إطار قانوني محدد، كحماية الحقوق المتعلقة بالملكية الفكرية، وحتى في هذا الإطار فلا يمكن أن تكون هذه الأعمال محلا للسرقة ، لأن هناك جريمة أخرى تنطبق على مثل هذه الحالة وهي التقليد[3].

2) أن المعلومات قد تكون لعدد لا حصر له من الملكيات المتماثلة، وهو ما يتنافى مع فكرة المال على الشيوع الذي يفترض انحصاره في عدد محدد من الأشخاص[4].

الخلاصة:-

وبناء على ما سبق ومن خلال الإطلاع على الخلافات الفقهية بصدد محل جريمة السرقة، فإننا نؤيد أصحاب الاتجاه الذي يرى أن المعلوماتية مال منقول مملوك للغير، وإن خالفناهم في رأيهم المتمثل بأن المال له طبيعة معنوية وليست مادية، ومع ذلك فإن

(1) أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص483 وما بعدها.
(2) راجع أحمد خليفة الملط، مرجع سابق، ص306، هدى حامد قشقوش، مرجع سابق، ص59.
(3) نائلة عادل محمد فريد قورة، مرجع سابق، ص156.
(4) Vergucht (Pascal), La Répression des Délits Informatiques dans perspective Internationale, Thèse, Université de Montpellier I, 1996, p. 109
مشار إليه لدى نائلة عادل محمد فريد قوره، المرجع السابق، ص156.

خضوع المعلومات للقواعد العامة في جريمة السرقة رهين بتحقق باقي أركان الجريمة وملا أمتها للانطباق على سرقة المعلوماتية للاتي:

1) لو لم نعتبر المعلوماتية أموالا لما كان لها القيمة الاقتصادية التي لا يستطع أحد أن ينكرها، فقد أصبحت سلعة تباع وتشترى، بل إن الثورة التي نعيشها هي بالأساس ثورة معلومات، تتسابق الدول على اقتنائها، بل وتتنافس الشركات عليها لما لها من قيمة اقتصادية، كما أن اعتبار الكيان المادي للدعامة التي تحوي المعلومة مبررا للتجريم أمر لا يبدو مقبولا، فالقيمة الضئيلة للدعامة مقارنة بالقيمة المرتفعة للبرنامج تجعل من المنطقي والمعقول اعتبار المال في المعلوماتية لا الدعامة.

2) أن المعلومات إضافة إلى اعتبارها مالا - سواء اعتبرت مالا ماديا أم معنويا- هي قابلة لأن تنقل من شخص إلى آخر، فالمعلومات والبرامج تعتبر مالاً منقولاً تنتقل حيازته من مالكه إلى الغير، ويخضع للتصرفات التي تخضع لها سائر الأموال، وبناء على ذلك فعندما يحدث اعتداء على تلك الأموال المعلوماتية بنسخها أو سلب حيازتها، بحيث تصبح في حوزة المتهم فذلك يدل على أنها منقولات، قد انتقلت من مالكها إلى الغير بطريقة غير شرعية.

3) إخضاع الأمر للتحليل المنطقي يقتضي بأن تكون المعلومات مملوكه لشخص ما له حق الاستحواذ عليها والتصرف فيها، لما تمثله من قيمة اقتصادية لمالكها.

ثانيا: الركن المادي لجريمة السرقة في مجال المعلوماتية

يتمثل الفعل الذي يقوم عليه الركن المادي في جريمة السرقة بالاختلاس -وفقا للقواعد العامة- ويقصد به " الاستيلاء على حيازة شيء بغير رضا مالكه أو حائزه"[1]، فيتحقق فعل الاختلاس إذا ما قام الجاني بحركة مادية ينقل بها الشيء إلى حيازته بأي طريقة كانت، سواء بالنزع، أم السلب، أم الخطف، أم النقل، وما إليها، على أن يتم الاستيلاء بفعل الجاني، وليس من الضروري بيده، بل بواسطة أشياء أخرى خاصة بالجاني.

و يقوم فعل الاختلاس على عنصرين: أحدهما موضوعي، والآخر شخصي، والعنصر الموضوعي يتمثل بالنشاط الذي يصدر من الجاني ويؤدي إلى نتيجة معينة،

---

(1) حسني الجندي، مجدي عقلان، مرجع سابق، ص167.

أما العنصر الشخصي فيتمثل في نية تملك الشيء محل الاختلاس من قبل الجاني وعدم رضا المجني عليه بالاستيلاء على ماله، وسيتم إيضاح عنصري الاختلاس الموضوعي والمعنوي، إضافة إلى أثر التسليم على فعل الاختلاس - بنوع من الإيجاز- ومدي تحقق ذلك في نطاق المعلوماتية:

1- فعل الاختلاس واثر التسليم عليه وفقا للقواعد العامة

وفي هذا الموضع سيتم إيضاح عناصر فعل الاختلاس وأثر التسليم على فعل الاختلاس.

أ- عناصر فعل الاختلاس

1) العنصر الموضوعي للاختلاس

نظرا لخلاف الفقهاء حول تحديد معنى الاختلاس بصوره دقيقة، فقد وجدت العديد من النظريات التي تحدد معنى الاختلاس، وذلك بهدف تدارك القصور.

فبداية ظهرت **النظرية التقليدية** التي اقتصرت على تحديد فعل الاختلاس بانتزاع أو أخذ المسروق أو نقله لدى الجاني بدون رضا المجني عليه، باعتبار أن السرقة جريمة لها ذاتيتها القانونية، وذلك ما يميزها عن النصب وخيانة الأمانة، لعدم تحقق النزع أو النقل للشيء في هاتين الجريمتين، بل إن تسليم المال فيهما يتم من قبل المجني عليه، إلا أن تلك النظرية لم تسلم من المثالب، ومنها : استبعاد وقوع فعل الاختلاس إذا لم يتم بأفعال إيجابية صادرة من الجاني، وبالتالي فتطبيق تلك النظرية لا يؤدي إلى تجريم الأفعال التي لا تحتاج إلى حركة مادية لاقترافها مثل سرقة الكهرباء، وكذلك إعفاء الجناة في حالة ما يتم تسليم الشيء لهم من قبل المالك[1]، وبسبب قصور تلك النظرية ظهرت نظرية أخرى، وهي نظرية التسليم الاضطراري.

ونظرية التسليم الاضطراري: تقوم على أن التسليم الذي تم بصورة اضطرارية، ثم لا يقوم من تسلم الشيء بإعادته إلى مالكه فإنه يعد سارقا، ومثال ذلك من يقوم بفحص الشيء الذي يريد شراءه ثم لا يقوم بإعادته. وهذه النظرية كسابقتها ظهرت لها بعض العيوب ومنها: امتداد تجريم السرقة إلى بعض الأفعال التي لا يصدق عليها هذا

---

(1)عبدا لله حسين محمود، مرجع سابق، ص253.

الوصف، مثل الذي يأكل بالمطعم، ثم يمتنع عن دفع الحساب، فوفقا لهذه النظرية يعتبر التسليم اضطرارياً مع أنه تم برضا صاحب الشيء .

كما أن تطبيقها يؤدي إلى نتائج غير منطقيه في بعض الحالات ومثال ذالك امتناع الشخص الذي تسلم من صديقه شيئا عن رد ذلك الشيء وفراره به [1]، وذلك ما دفع المشرع الفرنسي إلا تجريم مثل تك الحالات بنصوص خاصة. وإزاء ذلك القصور فقد ظهرت النظرية الحديثة، حيث قامت قامت هذه النظرية على أساس الموازنة بين الجريمة والعقاب، وربط الحيازة بالاختلاس، فقد عرفت الاختلاس "بأنه الاستيلاء على الحيازة الكاملة للشيء بعنصريه المادي والمعنوي بدون رضا المالك أو الحائز " [2].

فيتحقق فعل الاختلاس بإخراج الشيء من الحيازة الكاملة للمالك أو الحيازة الناقصة للحائز، أو استخلاصه من صاحب اليد العارضة، ثم إدخاله في حيازة الجاني الكاملة أو حيازة غيره [3].

2) العنصر المعنوي في فعل الاختلاس

يتمثل العنصر المعنوي في الاختلاس بعدم رضا المالك أو الحائز للشيء باختلاس ما يملكه من أشياء، بل يجب أن يقع رغماً عن إرادته، ومع أن هذا الشرط لم يرد صراحة في القانون، إلا أن فكرة الأخذ خفية تتطلب تحققه [4].

ويترتب على شرط عدم رضا المالك كشرط لتحقق فعل الاختلاس بأنه إذا توافر الرضا من صاحب الحق بأخذ الشيء الذي يملكه فإنه تبعا لذلك ينتفي ركن الاختلاس، شريطة أن يكون الرضا سابقا على فعل الاختلاس أو معاصرا له ، بعكس الرضا اللاحق للفعل حيث لا يؤثر على قيام الجريمة.

ب- التسليم وآثاره في الاختلاس

يعتبر التسليم الذي يتم من المالك أو من الحائز نافيا للاختلاس متى ما تم من أي منهم بالتنازل عن الحيازة الكاملة أو الناقصة، ويترتب على ذلك أن التسليم من صاحب اليد العارضة لا يكون نافيا للاختلاس لعدم وجود سلطه على المال .

---

(1) عفيفي كامل عفيفي ، مرجع سابق، ص129.
(2) أحمد خليفة الملط، مرجع سابق، ص272.
(3) عبد الله حسين محمود، مرجع سابق، من ص257 وحتى ص259.
(4) حسني الجندي، شرح قانون العقوبات اليمني، مرجع سابق، ص 196.

كما أن التسليم الذي يتم به نقل الحيازة الكاملة أو الناقصة ويعد نافيا للاختلاس هو التسليم الذي يتم بموجب الطرق القانونية، وبموجبه فقد قضى "بأنه إذا كان من الثابت بالحكم أن المتهم تسلم السند ليعرضه على شخص ليقرأه له في نفس المجلس ويرده في الحال ثم على اثر تسلمه إياه أنكر في نفس المجلس فإنه يعد سارقا "(1).

والتسليم الذي يكون نافيا للاختلاس لابد وان يصدر عن أرادة حرة وواعية يعتد بها في القانون، وبالتالي فإنه لا ينتفي الاختلاس في حالة التسليم من المكره أو المجنون أو المعتوه، بعكس التسليم المبني على غلط أو غش أو تدليس فإنه ينفي الاختلاس كونه صادر عن أراده حرة ومدركه (2).

2- مدى تطابق فعل الاختلاس في مجال المعلوماتية مع القواعد العامة للسرقة

تم إيضاح الركن المادي للسرقة وفقا للقواعد العامة بنوع من الإيجاز، وذلك بهدف الوصول إلى نتيجة مفادها هل بالإمكان تطبيق تلك القواعد على الركن المادي في مجال المعلوماتية؟ بمعنى آخر هل عناصر الركن المادي في جريمة السرقة وفقا للقواعد العامة هي نفس عناصر الركن المادي للجريمة في مجال المعلوماتية حتى يمكن القول بتطبيق نصوص القانون التقليدي؟ وما هي أوجه الربط أو العلاقة التي يمكن استنباطها؟ وهل التسليم وآثاره وفقا للقواعد العامة هو نفس التسليم في مجال المعلوماتية؟ ذلك ما سيتم دراسته في هذا الموضع:

أ- عناصر فعل الاختلاس في مجال المعلوماتية

1) العنصر الموضوعي لفعل الاختلاس

يتمثل العنصر الموضوعي لفعل الاختلاس بالنسبة للمعلوماتية بالاستيلاء على البرامج والبيانات المعالجة آليا، إلا أن الاستيلاء على المعلوماتية قد يتم بصور حديثة أظهرها التقدم التكنولوجي، ومنها الالتقاط الذهني للبيانات، والنسخ غير المشروع للبيانات المخزنة في النظام، والالتقاط الهوائي للبيانات المعالجة والمنقولة وسيتم التطرق إليها تباعا لإيضاح مدى تطابق العنصر الموضوعي لفعل الاختلاس لكل صوره على حدة، مع القواعد العامة التي تحكم الفعل في حالة استخدام الوسائل التقليدية، وبمفهوم

(1) نقض مصري 1945/3/19، مجموعة القواعد القانونية، ج6، ق524 ص663 ، مشار إليه لدى أحمد خليفة الملط، مرجع سابق، ص276 .
(2) راجع: حسني الجندي، ومجدي عقلان، مرجع سابق، ص174 وما بعدها.

آخر هل نقل الحيازة للمعلوماتية من المجني عليه إلى الجاني بنية التملك وبدون رضا المجني عليه يمكن أن تشكل العنصر الموضوعي لفعل الاختلاس في جريمة السرقة، لكي يمكن القول بانطباق النصوص القانونية الخاصة في جريمة السرقة؟

أ) الالتقاط الذهني للبيانات

تتم عملية الالتقاط الذهني للبيانات بالاختزان والحفظ الواعي أو العرضي للمعلومات في ذاكرة الإنسان أثناء مطالعته لها بالبصر، إن كانت قد ظهرت على شاشة الحاسوب في شكل مرئي، أو بعد وصولها إلى الأذن حينما تأتي على شكل أصوات صادرة من الأجهزة[1].

والالتقاط الذهني للبيانات عن طريق البصر يقع تحت طائلة الاختلاس، ومن ثم يخضع لعقوبة السرقة لمبررات يراها أصحاب هذا الاتجاه وهي:

1- أن الاستيلاء على المعلومة عن طريق السمع والمشاهدة يتحقق به فعل الاختلاس في جريمة السرقة إذا ما تم تفريغ المعلومات من الذاكرة إلى إطار مادي وتحييزها فيه والاستئثار بها، وهي بذلك تمكن حائزها من نقلها من ذمته المالية إلى ذمة أخرى في حالة بيعها، أما إذا ظلت حبيسة الذاكرة دون تسجيلها فلا تقع تحت طائلة العقاب[2].

2- بالإمكان نقل حيازة المعلومة من الجهاز إلى ذهن المتلقي لكون موضوع الحيازة أي المعلومات غير مادي، فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية(ذهنية)، وبالتالي يمكن حيازة المعلومات عن طريق الالتقاط بالبصر أو السمع وهو المقصود من جانب الجاني، كما أن التيار الكهربائي قابل للانتقال بالرغم من عدم حيازته المادية، فكذلك الشيء المعلوماتي (3).

3- أن البرامج والمعلومات المعالجة آليا طالما تم وضعها والتعامل فيها فإنها تصبح مالية ومادية، وبالتالي تصلح لأن تكون محلا للاختلاس، سواء تم نقلها أم

---

(1) راجع هشام فريد محمد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص232.

(2) Lucas de Leyssacl (Marie - paul), une information seule est susceptible de value d'une autre atteinte juridique aux biens , p. 198, chronique , n 36 , p. 49 ; kessler (Michel) ,le logiciel , protection juridique France et étranger, p. 57et 60
مشار إليه لدى أحمد خليفه الملط ، مرجع سابق، ص318 .

(3) هدى حامد قشقوش، جرائم الحاسوب الالكتروني في التشريع المقارن، مرجع سابق، ص56، وص57.

نسخها أم الاطلاع عليها بالبصر أم السمع، بمعنى آخر طالما أن المعلومات التي يتم التقاطها ذهنيا تسبب الضرر لمالكها وبقيمتها الاقتصادية، إذا ما قام الجاني باستخدامها وترجمتها على شكل مخرجات، سواء باسطوانات أم شرائط أم أوراق، وعرضها للبيع وبالتالي تصلح لأن تكون موضوعا للاختلاس[1].

- عدم قابلية المعلومات التي يتم التقاطها ذهنيا للاختلاس

1- لعدم وجود أي نشاط مادي أثناء الالتقاط الذهني للمعلومات، وأن تجريم أفعال أو جرائم تتمثل مادياتها في نشاط ذهني محض يؤدي إلى تجريم ما يدور في العقول والأذهان، وهو أمر غير مقبول[2].

2- لأن التجريم منذ زوال السيطرة الدينية التي سادت التشريع الجنائي في أوروبا خلال العصور الوسطى لا يلحق إلا النشاط المادي الذي يمكن لمسه بالحيز الخارجي على أي وجه من الوجوه، ومجرد الالتقاط الذهني - خلافا لالتقاط صورة الدعامة أو الوعاء الذي يحويها أو نقل محتواه عن طريق البث التلفزيوني - لا تتوافر فيه مقومات النشاط المادي ذي المظاهر الخارجية [3].

3- أن الصورة التي تظهر على شاشة النظام المعلوماتي وإن كانت تبدو في نشاط إنساني يمكن تقديره بالجهد الفني الذي يبذله المختص، إلا أنها لا تعتبر مكتوبة بالمرة، ولا تصلح للسرقة[4].

---

(1) أحمد خليفه الملط، مرجع سابق، ص319. والرأي المشار إليه في البند (3) هو رأي الدكتور الملط بعد الترجيح بين الرأي القائل بصلاحية الالتقاط الذهني للبيانات لفعل الاختلاس في جريمة السرقة والرأي القائل بخلاف ذلك.

(2)هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص234.

(3) هشام محمد فريد رستم، نفس المرجع، ص233 . وقد أكد رأيه بالحكم الذي أصدرته المحاكم الإنجليزية في قضية (Oxford v .Moss) سنة 1978 ببراءة مهندس كان يدرس في جامعة ليفربول من تهمة السرقة التي وجهت إليه لقيامه بالاستيلاء على نسخه من ورقة أسئلة امتحانات مادة الهندسة المدنية قام بالاطلاع عليها ومن ثم إعادتها بعد ذلك، وتأسس هذا الحكم على أن كشف المعلومات التي تحويها ورقة الأسئلة لا يتحقق به سرقتها لأن المعلومات ليست من أشكال الأموال المحسوسة.

(4) ومن التطبيقات القضائية التي تؤكد عدم قابلية المعلومات التي يتم التقاطها ذهنيا للاختلاس حكم محكمة باريس فيما يتعلق بالاختلاس الناتج عن الالتقاط غير المشروع الوارد بقضية قناة التلفزيون في فرنسا والمسماة بـ (canal plus) من أن فكرة الاختلاس لا تتم من خلال الاعتداء على العنصر المادي للشبكة المنتجة للبرامج التي تبث بوضوح وتلك التي تبث مشوشة، فقد اعتبرت المحكمة بعدم توافر عناصر جريمة السرقة لأن التوصل غير المشروع لالتقاط برامج القناة لم يكن من شأنه أن يغل يد مالك البرنامج عنه، ورأت المحكمة في حيثيات الحكم عدم توافر جريمة السرقة. راجع; أحمد خليفة الملط، مرجع سابق، ص316، وص317.

ب) النسخ غير المشروع للبيانات المخزنة إلكترونيا

هذه الصورة تتمثل بتخزين البيانات المعالجة إلكترونيا على هيئة نبضات كهربائية في دوائر إلكترونية مجمعة أو على أشرطة أو اسطوانات ممغنطة، وفي الحالتين يمكن نسخها على دعامات أخرى، فهل يمكن تطبيق أحكام السرقة على عملية النسخ، بمعنى آخر هل يتحقق بنسخ المعلومات ركن الاختلاس في جريمة السرقة ؟

وبهذه المسألة يرى البعض، عدم قابلية المعلومات المنسوخة بذاتها للسرقة بينما يرى البعض الأخر قابليتها للسرقة:

عدم قابلية المعلومات للسرقة

1- لانتفاء الصفة المادية للبيانات المخزنة إلكترونيا في الدعامات، كونها صفه يجب أن تتوافر في المحل الذي تنصب عليه السرقة وهي الدعامات [(1)].

2- أنه يترتب على سرقة المعلومات والبرامج من على الدعامة أضرار تفوق قيمة الدعامة ذاتها، ويرجع ذلك إلا أن اختفاء المعلومات يعقبها إفشاء الأسرار التي كان يتوقع بقاؤها في نطاق الأسرار، ويمكن العقاب عليها كجريمة إفشاء الأسرار[(2)].

3- أنه في حالة افتراض وقوع الاختلاس على الأشياء المعنوية فيجب أن يقابله تشدد في تحقيق طبيعة هذا الاختلاس، بضرورة تحققه في نشاط مادي بان ينقل على دعامة مادية، فاخذ شيء غير مادي مثل المعلومات لا يكون ماديا إلا إذا تجسد في هيئة مادية[(3)].

4- يؤكد بعض الفقهاء اتجاه القضاء في توفير الحماية القانونية للمعلومات، على الرغم من أنها من الأموال ذات الطابع المعنوي، فقد اتجهت أحكام قضائية إلى القول بوقوع جريمة السرقة مادامت المعلومات مسجلة على دعامة مادية [(4)].

---

(1)أحمد خليفة الملط ، مرجع سابق، ص319 .
(2) نائلة محمد فريد قوره، مرجع سابق، ص146.
(3) ورد هذا الرأي في مؤلف آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص25.
(4) غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 1- 3 مايو 2000م، ج2، ط3، ص 634.

- **أن الأشياء المعنوية والمعلومات المنسوخة تخضع لنص السرقة**

1- لأن المعلومات يمكن حيازتها إذا حواها وعاء، ومن ثم يمكن سلب حيازتها، ويجوز بالتالي أن تكون محلا للسرقة طالما أن نسخها يتم من خلال نشاط مادي يتمثل في النسخ أو التصوير، ونقلها على دعامة مادية [1].

2- لأن لفظ شيء في القانون الفرنسي لم يفرق بين الأشياء المادية والأشياء المعنوية، فلم يقتصر على الماديات فحسب بل إنه يشمل الأشياء غير المادية[2].

3- لأن الدعامة تعتبر عديمة القيمة بدون المعلومات، وبالتالي فإن المعلومات المخزنة على دعامات تصلح لأن تكون محلا للاختلاس باعتبارها مالاً منقولاً ولها قيمة اقتصادية[3].

4- أن أغلب الأحكام التي صدرت في فرنسا أيدت الرأي الثاني[4].

ج) الالتقاط الهوائي للبيانات المعالجة أو المنقولة إلكترونيا

في هذه الصورة يتم التقاط البيانات أو المعلومات من جهاز الحاسوب أثناء تشغيله إضافة إلى ذلك، فقد يتم اعتراض المعلومات والبيانات أثناء نقلها بالموجات القصيرة من نهاية طرفيه إلى نهاية أخرى[5]، فما مدى صلاحية تلك الموجات والإشعاعات لأن تكون محلا للسرقة ؟

الراجح في الفقه بأن الموجات أو الإشعاعات المنبعثة من الأجهزة أثناء تشغيلها وإن صلحت بسبب تجسدها في صورة مادية كهرومغناطيسية لأن تكون محلا للسرقة،

---

(1) Lucas de Heyssac: une information seule est elle susceptible de vol, article précité.

مشار إليه لدى آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص40.

(2) محمود أحمد عباينة: جرائم الحاسوب وأبعادها الدولية، رسالة ماجستير، دار الثقافة للنشر والتوزيع،عمان، 2005، ص98.

(3) أحمد خليفة الملط ، مرجع سابق ، ص220.

(4) ومن تلك الأحكام : ما قضت به محكمة جنح(Montbéliard)بإدانة موظف سابق بشركة بيجوت بجريمة السرقة وليس التقليد ، لقيامه بعد استغناء الشركة عنه بالعودة إلى مقرها، ومن ثم نسخ مجموعة برامج معلوماتية تخص الشركة على اسطوانة ممغنطة، حيث جاء في الحكم أن المتهم قد استولى وحاز دون أن تكون الحيازة قد انتقلت إليه تسجيلا لمعطيات وإن كان قد أسهم بمعلوماته في إعدادها إلا أنها تخص رب العمل.راجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، 243.

(5) ومن الأمثلة التي ورد ت للالتقاط الهوائي للبيانات و المعلومات قيام فيم فإن ايك (وهو مهندس في إدارة الخدمات البريدية والهاتفية والبرقية في هولندا) بتجميع جهاز تلفزيوني صفير وهوائي ومنظومة دارات كهربائية، بقصد التصنت على الاتصالات المتبادلة بين عدد من المؤسسات الأوربية، وقد نجح في التقاط إشارات من حاسب إلكتروني في مجمع مكتب يقع في الطابق الثامن من أحد الأبنية، كما استطاع التقاط إشارات من الحاسوبات الإلكترونية لبنك عبر أحد الشوارع العريضة. راجع هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ص250 .

إلا أن التقاطها لا يتحقق به معنى انتزاع أو سلب حيازتها فلا تقع جريمة السرقة لانتفاء أحد عناصر الركن المادي، والأمر كذلك بالنسبة لاعتراض البيانات المعالجة إلكترونيا أثناء تناقلها، إرسالا واستقبالا بين الأجهزة المعلوماتية.

فقد قضت محكمة باريس في واقعة فك احتيالي لشفرة إرسال تلفزيوني يتم استقباله نظير رسم، بأن " الموجة الهرتيزية سواء كانت حاملة لإشارة مكودة أم لا، تنطلق في الفضاء حيث تضيع، وهكذا تفلت، بدءا من هوائي الإرسال، من سيطرة مرسلها "، ولا يمكن من ثم أن تكون موضوعا للسرقة[1].

2) العنصر المعنوي في فعل الاختلاس

كما أن العنصر المعنوي في فعل الاختلاس في جريمة السرقة وفقا للقواعد العامة هو عنصر مفترض، فهو كذلك بالنسبة لصاحب الحق على الشيء المعلوماتي المعنوي، فمالك الشيء - بلا شك- غير راض باختلاس ما يملك من أشياء معلوماتية، و يتطلب العنصر المعنوي في الاختلاس أن يكون لدى الجاني نية في تملك الشيء المختلس .

كما أن القواعد التي تتعلق بالرضا النافي للاختلاس والتي سبق إيضاحها وفقا للقواعد العامة والتي منها: أن يكون الرضا ناتجا عن أراده حرة ومدركة، وأن يكون من شخص له صفه على الشيء كالمالك أو الحائز، وان يكون صادراً قبل الاختلاس أو معاصرا له، ومن ثم لا يعتد بالرضا اللاحق، كل تلك الأحكام يمكن أن تنطبق على سرقة المعلوماتية .

ب- التسليم الواقع في مجال المعلوماتية وأثره على فعل الاختلاس

وجد أن الخلاف في مجال التسليم في نطاق المعلوماتية قد انصب على موضوع التسليم الصادر من جهاز التوزيع الآلي للنقود بشأن الشخص الذي حصل على مبالغ نقدية أكثر من الحد المسموح له ببطاقة الائتمان[2] . فهل التسليم الذي صدر من جهاز

(1) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ص 253، وص254.

(2) نتج عن التقدم التكنولوجي الملموس وانتشار أنظمة المعلوماتية وظهور الشبكات ودخولها إلى عالم المعلوماتية بالبنوك والمؤسسات المالية والتجارية إلى إيجاد وسائل تتناسب مع التعاملات السريعة عبر بنوك المعلومات، وهي بطاقات الائتمان أو الوفاء-الفيزا كرت- وهذه البطاقات سهلت المعاملات بصورة لم تكن متوقعة بين البنك والعميل، سواء عن طريق سحب مبالغ مالية عبر أجهزت السحب الآلية، أو الوفاء بقيمة المشتريات التي قام بها العميل من المؤسسات التجارية التي تتعامل بها، إلى غير ذلك من الخدمات التي أضحى الشخص بموجبها لا يتكلف في حمل النقود حتى أثناء سفره، وأصبح يغني عن ذلك حمل مثل تلك البطاقات ذات الطابع الدولي في التعامل، إلا أنه ومع كل تلك الخدمات فقد ظهرت العديد من المخاطر بسبب تلك التكنولوجيا، وذلك بقيام صاحب البطاقة باستخدامها استخداما تعسفياً، أو غيره في حالة فقدها أو سرقتها وسحب مبالغ أكثر من الرصيد المسموح به، أو التعامل بها بعد أن أصبحت ملغاة أو منتهية إلى غير ذلك من الجرائم .راجع أحمد خليفة الملط ، مرجع سابق ، ص323.

التوزيع الآلي للنقود يعد نافياً للاختلاس؟ وما هو التكييف القانوني للتسليم في مثل هذه الحالة؟

انقسم الفقه بشأن واقعة التسليم الصادرة من جهاز التوزيع الآلي للنقود التي بمقتضاها تم تسليم العميل أكثر من الرصيد المسموح به إلى اتجاهين:

فالبعض يرى وصف الفعل بأنه سرقة للمبررات الآتية:

1) تشبيه حالة العميل الذي يقوم بسحب مبالغ تتجاوز رصيده بواسطة بطاقة الائتمان من جهاز السحب الآلي بالدائن الذي يقدم له مدينه حافظة نقوده لكي يأخذ منها الدين المستحق له، فيستولي على أكثر من حقه، وبدون رضا المدين، وعلى ذلك يعد الفعل سرقة[1].

2) أن التسليم الذي يتم زيادة عن رصيد الساحب، هو تسليم لم يتم عن طريق الخطأ، فالآلة المجردة عن الإرادة والتفكير لا يمكن أن ترتكب خطأ بالمعنى القانوني[2]

3) ويؤيد الرأي السابق من جانب الفقه العربي[3]، بخضوع العميل الذي يتجاوز السحب عن رصيده من جهاز السحب الآلي لعقوبة السرقة، فالعبرة هي إذن بمضمون العقد الذي يوجد بين العميل والبنك، ويمكن للبنوك تعديل الالتزامات التي تفرضها على العملاء في حالة السحب من أجهزة التوزيع الآلي للنقود بأن تفرض عليهم عدم السحب فيما يجاوز الرصيد، وبالتالي يسأل العميل عن جريمة سرقة في حالة تجاوزه بالسحب أكثر من رصيده.

والبعض الأخر يرى بأن الفعل لا يمكن وصفه بالسرقة للأسباب التالية:

1) أن التسليم قد تم عن طريق الرضا، حيث وأن منافذ التوزيع تعمل وفقا لأوامر البنك، بموجب برنامج كان من المفترض أن لا يمكن الساحب من سحب مبالغ تتجاوز رصيده، حيث أن البطاقة التي يتكرر إدخالها ومحاولة السحب بها لأكثر من

---

(1) مشار إلى هذا الرأي في مؤلف أحمد خليفة الملط ، مرجع سابق، ص327، وكذلك في مؤلف جميل عبد الباقي الصغير، الحماية الجنائية لبطاقات الائتمان الممغنطة، مرجع سابق، ص52، وهو يخالف هذا الرأي باعتبار أن هذا الرأي قد استند إلى حكم قضائي فرنسي بتاريخ 21 ابريل 1964 اعتبر أن أخذ الدائن من محفظة مدينة أكثر من المبلغ المستحق كدين يعد جريمة سرقة، وقياس حالة السحب من جهاز الصراف الآلي أكثر من الرصيد على هذه الحالة أمر غير منطقي لأن السرقة في الحالة الأولى تمت بعد القيام بالتسليم، أما في حالة السحب من جهاز الصراف فإنه يتم بهدف الحصول على التسليم، كما أن العميل في الحالة الأخيرة يقع في الغلط نتيجة لضنه أنه يتمتع بنوع من التسهيلات البنكية.

(2) مشار إليه في مؤلف أحمد خليفة الملط، مرجع سابق ،ص 328.

(3) أحمد خليفة الملط، مرجع سابق، ص129.

ثلاث مرات يقوم الجهاز بسحبها، لكن تجاهل البنك يجعل من التسليم الذي لا يكون ناتجا عن محاولات احتيالية تسليما نافيا للاختلاس (1).

2) ويؤيد هذا الرأي(2) وذلك باستبعاد تكييف قيام العميل بالسحب من جهاز الصرف الآلي متجاوزا رصيده بجريمة السرقة، فوجود عنصر الرضا الذي يتصور وجوده في هذه الحالة، إضافة إلى الغلط الذي يقع فيه المتهم ظانا أنه يتصرف في نطاق حقه، أو أن ذلك نوع من التسهيلات البنكية فالكثير يخلط بين بطاقة الوفاء وبطاقة الائتمان، هذه العناصر وغيرها تجعل من الصعب قياس حالة السحب من الآلة على حالة الدائن الذي يستولي على حافظة نقود مدينه(3).

3) التأكيد على اتجاه محكمة النقض الفرنسية بهذا الشأن وذلك بعدم إضفاء أي طابع إجرامي على هذا الفعل، معتبرةً أن الأمر لا يعدو أن يكون مجرد إخلال بالتزام تعاقدي، ولا ينطوي على أي جريمة جنائية لعدم وجود نص يجرم هذا الفعل (4).

ثالثا: الركن المعنوي لجريمة السرقة في مجال المعلوماتية

يقصد بالركن المعنوي مجموعة العناصر النفسية والذهنية التي يسهم بها الشخص في ارتكاب الجريمة (5).

فالواقعة غير المشروعة لا توصف بأنها جريمة جنائية، ولا تستند جنائيا إلى من أحدثها، إلا إذا وجدت رابطة نفسية ذهنية تصل بينها وبين الفاعل، وهذه الرابطة هي جوهر الركن المعنوي.

وتكمن العناصر النفسية التي يقوم عليها الركن المعنوي للجريمة على عنصري العلم والإرادة، إلا أن بعض الجرائم ومنها جريمة السرقة تتطلب إضافة إلى القصد

---

(1) Lucas de Leyssac V . ègalement , Avectautes les ref . a la jurisprdence et a la doctrine antérieur , le commentaires de bauzat , rev scince crime 1984 , 416 ; Cabrilac et Teyssie , rev . trim . dr . com Sousiroubi , gez . pel 16au 18dec . 1984 , D, 2, Vasseur .D.1984 , LR , 307
مشار إليه لدى أحمد خليفة الملط ، مرجع سابق ، ص 325.

(2) عمر سالم، الحماية الجنائية لبطاقة الوفاء، ط1، دار النهضة العربية، القاهرة،1995، ص47.

(3) عمر سالم، المرجع السابق، ص 49، وراجع جميل عبد الباقي الصغير، الحماية الجنائية لبطاقات الائتمان الممغنطة، مرجع سابق، ص53.

(4) مشار إليه في مؤلف عفيفي كامل عفيفي، مرجع سابق، ص158، وجميل عبد الباقي الصغير، الحماية الجنائية لبطاقات الائتمان الممغنطة، مرجع سابق، ص58.

(5) علي حسن الشرفي، شرح الأحكام العامة للتشريع العقابي اليمني وفقا لمشروع القانون الشرعي للجرائم والعقوبات، دار المنار، القاهرة، 1993، ص318.

الجنائي العام المتمثل بالعلم والإرادة توافر قصد جنائي خاص، كونها من الجرائم العمدية التي يجب أن يتوافر لدى المتهم القصد الجنائي بنوعيه العام والخاص[1].

- **القصد الجنائي وفقا للقواعد العامة**

يعتبر القصد الجنائي في جريمة السرقة متحققا - وفقا للقواعد العامة- بعنصريه العلم والإرادة، متى كان الجاني يعلم بأنه يقوم بعمل غير مشروع، وأن المال الذي يقدم على اختلاسه هو مال يخص غيره، وأنه بإقدامه على ذلك الفعل سواءً قام بنقل أم تحويل الحيازة من المالك الأصلي للمال إليه ليصبح ضمن أملاكه وتحت سيطرته.

و يجب أن يكون الجاني عالما بأن تلك الأفعال ستتم بدون رضا صاحب المال، وأن المال الذي يقوم باختلاسه ليس ملكا له، وبالتالي فإن جريمة السرقة تنتفي في حالة أن يقوم الفاعل بسرقة مال هو في الحقيقة ملكا له، حتى لو لم يدرك ذلك أثناء اقترافه للفعل، كأن يعلم بعد قيامه بأخذ المال بأن المال المأخوذ هو ملكه من مورثه، كما أن السرقة تنتفي في حالة أن يكون أخذ المال قد تم برضا صاحبه.

فعنصر العلم يقتضي أن يكون الجاني عالما بعناصر الركن المادي للجريمة إضافة إلى عناصر الركن الشرعي، إلا أن العلم بالركن الشرعي هو شيء مفترض لا يقبل إثبات العكس، فالعلم بالنصوص القانونية هو علم مفترض لا يقبل الدفع بخلافه، ولا يحتاج إثباتاً في قيامة، بخلاف العلم بعناصر الجريمة حيث يحتاج إلى إثبات بقيام ذلك العلم، ولا يمكن الجزم بوجوده حتى يقوم الدليل عليه [2].

أما العنصر الآخر من عناصر الركن المادي في جريمة السرقة فهو عنصر الإرادة، والإرادة هي عبارة عن نشاط نفسي اتجه إلى تحقيق غرض عن طريق وسيلة معينة، وهي تمثل جوهر القصد وعنصره الأساسي، فالتسلسل المنطقي للعوامل النفسية يكون مبدؤه العلم الذي يفضي إلى الرغبة في الإقدام على العمل، وهذه الرغبة هي أم الإرادة [3].

---

(1) محمد أمين أحمد الشوابكة: الجريمة المعلوماتية، رسالة ماجستير، جامعة القاهرة، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004، ص160.
(2) علي حسن الشرفي، مرجع سابق، ص318.
(3) علي حسن الشرفي، مرجع سابق، 1993، ص370.

ولابد لتحقق الجريمة أن تنصرف الإرادة إلى كل العناصر المكونة للجريمة، فلابد أن تتجه إرادة الجاني إلى ارتكاب السلوك المكون للجريمة، ويكون ذلك نتيجة الرغبة الكاملة في اقتراف ذلك السلوك وفي تحقيق النتيجة التي تترتب عليه .

أما القصد الجنائي الخاص في جريمة السرقة فيتمثل بنية تملك المال المسروق، ونية التملك للمال المسروق تكون بالاستيلاء على المال المنقول المملوك للغير، بنية إضافته إلى ملك الجاني أو سلب حيازته نهائيا من الغير، وإدخاله في حيازة الجاني، والتصرف فيه تصرف المالك.

ونية التملك التي تتجه إليها إرادة الجاني هي عنصر آخر يضاف إلى عنصري القصد العام (العلم والإرادة) وليست من عناصر الجريمة، واشتراط هذه النية أو الرغبة الإضافية يدل على أن الجريمة لا تنهض إلا إذا توافرت تلك النية، فإذا تخلفت فقد تخلفت الجريمة .

وبناء على ذلك فلا تقع الجريمة إذا تم أخذ المال بقصد الاستعمال، ورده ثانية، لأن الاستعمال المؤقت لا يكفي في القصد الجنائي [1].

فإذا ما تحقق عنصر العلم والإرادة إضافة إلى نية التملك فإن جريمة السرقة تكون قد تحققت، بغض النظر عن الباعث لارتكابها، حتى لو كان الباعث شريفا كأن يقوم الفاعل باختلاس المال الذي يفي بحقه من مدينه خفية.

كذلك فإنه ينبغي أن يتوافر العلم والإرادة وقت حدوث النشاط الذي يصدر عن الفاعل، بغض النظر عن وقت حدوث النتيجة، فلا يؤثر تأخر حدوث النتيجة على القصد، طالما كان متوافرا وقت حدوث الفعل .

- **القصد الجنائي في جريمة سرقة المعلوماتية**

يتمثل القصد العام بعلم الجاني بالعناصر المكونة للجريمة، فيجب أن يعلم الجاني بأنه يقدم على فعل يجرمه القانون، ومن شأنه الاعتداء على المال المعلوماتي، سواء تمثل الفعل بالدخول إلى النظام المعلوماتي أم البقاء فيه، أم أي فعل آخر يتوصل به الجاني إلى سرقة المعلومات، كفعل الالتقاط أو الاعتراض للمعلومات أثناء تبادلها وانتقالها من نظام إلى آخر شريطة أن ينص القانون على تجريم تلك الأفعال، كما يجب

(1) أحمد خليفة الملط، مرجع سابق، ص 282.

أن يعلم الجاني أنه يقوم باختلاس معلومات مملوكة للغير، وبدون رضا مالكها، وبالتالي فإن القصد الجنائي ينتفي في حالة أن تكون المعلومات متاحة للكافة، أو أن يتم الاستيلاء عليها بموافقة مالكها، كما يجب أن تتوافر الإرادة باقتراف تلك الأفعال حتى يتحقق القصد الجنائي العام .

ويتمثل القصد الجنائي الخاص في سرقة المعلومات بتوافر نية التملك للشيء محل الاعتداء، فيعتبر القصد الجنائي الخاص متحققاً متى اتجهت إرادة الجاني إلى الاستيلاء على المعلومات، وتبديل حيازتها وممارسة سلطات المالك عليها. وبالتالي فإن اقتصار إرادة الجاني على مجرد حيازة الشيء حيازة ناقصة ينفي توافر القصد الجنائي الخاص[1].

ويجب أن تتزامن نية التملك والإضرار بالغير مع فعل الاختلاس، وبالتالي فإن الجريمة لا تقع في حالة ما يكون القصد الجنائي لاحقا لفعل الاختلاس [2]. كما أن الباعث لا يؤثر على قيام الجريمة، سواء كان شريفا أمدنيئاً طالما تحقق القصد الجنائي العام والخاص، فالذي يقوم بالدخول إلى نظام المعالجة الآلية للبيانات ويقوم بعمل تحويلات مالية تتساوى مع الذي لم يقم مدينة بالوفاء بها لا يستطيع أن يقدح بذلك الباعث اقترافه للجريمة.

رابعا: عدم ملائمة تكييف جريمة السرقة في مجال المعلوماتية.

سبق إيضاح نصوص القانون اليمني المتعلقة بالسرقة أثناء تناول السرقة في مجال المعلوماتية مقارنة بالقواعد العامة بنوع من الإيجاز، حيث تم الإيضاح بأن القانون اليمني قد أورد تعريفا لجريمة السرقة في نص المادة (294) ق.ع بأنها "أخذ مال منقول مملوك للغير من حرز خفيه".

وبموجب التعريف السابق يكون المشرع قد تطلب تحقق عدد من الشروط في جريمة السرقة وهي:

1- شروط تتعلق بمحل الجريمة، وتتمثل في أن يكون المسروق مالا، ويشترط في ذلك المال أن يكون منقولا وأن يكون ذا قيمة، وحدد قيمة المسروق بما يعادل قيمة نصف جنيه ذهب أبو ولد بالنسبة، للسرقة الحدية.

(1) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ، ص266.
(2) محمد أمين أحمد الشوابكة ، مرجع سابق ، ص161.

2- وشروط تتعلق بالركن المادي، وأهمها: أن يكون أخذ المال خفية عن مالكه، وأن يتم ذلك الأخذ من حرز.

فالركن المادي للجريمة يتمثل في أخذ المال خفية وذلك بأن يقوم الجاني بأخذ المال المسروق على سبيل الخفية والاستئثار دون علم المجني عليه ودون رضاه[1]، خلافا لمعظم القوانين التي تتطلب أن يتم الفعل باختلاس المال المنقول، بمعنى أن فعل الاختلاس يتم حتى لو كان صاحب المال على علم بذلك إذا لم يكن الاختلاس الذي تم بموافقته.

فإذا تحققت الشروط السابقة إضافة إلى القصد الجنائي العام والخاص فقد تحققت الجريمة، أما إذا لم تتحقق أركان الجريمة ولم يتوافر في فعل الجاني شروط الحد أو سقط الحد لأي سبب من الأسباب الموضحة في نص المادة (299) ع.ي، حتى لو كانت بالإكراه أو التهديد، أو اقتصرت على الشروع فإن الجاني يعاقب بعقوبة تعزيزيه[2].

وبذلك فإن القانون اليمني قد تناول جريمة السرقة في حالتها المادية، أي عندما تكون الأموال محل السرقة أموالاً مادية، ولم يتناول في نصوصه، أو بتشريع خاص الجرائم المعلوماتية بشكل عام، أسوة بأغلب التشريعات[3]، كما أنه لم يتضمن نصا يجرم سرقة المعلوماتية، مع أن القانون صادر في وقت أصبحت تلك الجرائم شائعة، ومناقشة

---

(1)عبدا لله أحمد فروان، أحكام السرقة بالتسبب في الشريعة والقانون، ط1، مكتبة الفاروق صنعاء،2004-2005، ص14.

(2) تنص المادة (300) ق.ع .ي بأنه (إذا ارتكب الفاعل جريمة سرقه ولا تتوافر في فعله شروط الحد أو سقط الحد لأي سبب من أسباب السقوط، إذا لم يصاحب الجريمة إكراه أو تهديد، يعاقب بالحبس مدة لا تزيد على ثلاث سنوات) وقد بينت المادة(299) الأسباب المسقطة للحد ومنها تملك الشيء المسروق بعد السرقة وقبل المرافعة أمام المحكمة، ونقص قيمة المسروق عن النصاب قبل تنفيذ الحد، وعفو أصحاب الحق قبل المرافعة أمام المحكمة، كما بينت المادة ذاتها الحالات التي لا تعتبر فيها جريمة السرقة حدية ومنها: حالة تعدد الفاعلين ولم يبلغ ما أخذه احدهم نصابا، وإذا حصلت السرقة بين الأصول والفروع، أو بين الزوجين، أو المحارم، وإذا كان مالك المسروق مجهولا، و إذا كان المسروق ثمارا من على الشجر أو ما يشابهها، وإذا رد الفاعل المسروق قبل الترافع إلى المحكمة، وإذا كان الفاعل دائنا لمالك المال بدين حال ثابت بحكم نهائي وكان المالك مماطلا، وكان المال الذي استولى عليه الدائن يساوي حقه أو يزيد عليه بما لا يساوي نصاب السرقة، وإذا حصلت السرقة من الأماكن العامة أثناء العمل فيها أو من أي مكان مأذون للفاعل بدخوله ما لم يكن المسروق محرزا.

(3) ويرجع الفراغ التشريعي لهذه الجرائم-حسب رأي نائب رئيس هيئة التفتيش القضائي لشؤون المحاكم ا لتجارية الدكتور القاضي علي سليمان - كونها جرائم مستحدثة، خصوصاً وأن اليمن في بداية التعامل الالكتروني، حيث أشار إلى أن اليمن يستخدم قانون العقوبات التقليدي الذي تحتوي نصوصه على النصب والاحتيال، لكن وزارة العدل بصدد الدراسة لإصدار قانون خاص بالجرائم الإلكترونية من خلال الاستعانة بالخبراء. راجع: علي سليمان، مقال منشور على موقع المحكمة التجارية اليمنية، ت.د 2008/3/9على الرابط:

http://www.qada.gov.ye/garymah.asp

من قبل الفقه والقضاء، وصدرت تشريعات بشأنها في العديد من دول العالم[1].و بالعودة إلى الفقه أو القضاء اليمني، يلاحظ عدم تعرض فقهاء القانون في اليمن لسرقة المعلومات ودور قانون العقوبات حيالها، مع أن بعضهم قد تعرض لاستخدام الوسائل الإلكترونية بغرض تحويل الأموال من البنوك بطرق غير شرعية، واعتبرها جريمة سرقه تنطبق عليها القواعد العامةفي قانون العقوبات اليمني معتبراً ذلك سرقة بالتسبب[2] . بينما اعتبرها البعض الآخر جريمة خيانة أمانة أو نصب[3].

و من تطرق لجريمة السرقة فقد اقتصر على الجانب المادي أو سرقة الأموال المادية وفقا لما كان معهودا من قبل[4].

إلا أنه ومن خلال المقارنة بين مؤيدي ومعارضي مدى خضوع سرقة المعلومات للنصوص التقليدية على ضوء الخلاف في مدى تطابق أركان جريمة السرقة وفق القواعد العامة مع القواعد الخاصة في مجال المعلوماتية، فيمكن إيضاح موقف القانون اليمني على ضوء ذلك، مع بيان بعض الأمور التي تتعلق بخصوصيته، ولا يضاح ذلك فيجب التفرقة بين الأموال المعلوماتية المادية والأموال المعلوماتية المعنوية.

أ- الأموال المعلوماتية المادية

الأموال المعلوماتية المادية مثل جهاز الكمبيوتر وتوابعه من الطابعة والأشرطة والسيد يهات وغيرها من الأموال المادية، فلا خلاف حول خضوعها لنص المادة (294) ق.ع، وهذه المسلة ليست محلاً للخلاف في الفقه أو القضاء وفقا لما سبق إيضاحه.

---

(1) مع أن قنون الجرائم والعقوبات اليمني لم يصدر إلى في وقت أضحت الجريمة المعلوماتية منصوصاً عليها في العديد من التشريعات العالمية، كما تم عقد العديد من المؤتمرات واللقاءات على مستويات دولية وإقليمية بشأنها، إلا أن المشرع اليمني لم يتنبه لذلك ويعمل على إضافة قسم في قانون العقوبات لمواجهة ذلك النوع من الإجرام، مع عدم إغفال جريمة السرقة في مجال المعلوماتية، وكذلك التزوير، ومع انه قد تم صدور قانون في عام 1998م بشأن مكافحة جرائم الاختطاف، والتقطع وألحق بقانون العقوبات، فلم يتم التنبه لما يتعلق بالجريمة المعلوماتية .

(2) عبدا لله أحمد فروان، مرجع سابق، ص 48.

(3) عبد المؤمن شجاع: جريمة التحويل الإلكتروني غير المشروع للأموال، مقال منشور على موقع المحكمة التجارية اليمنية، ت.د 2008/3/19 على الرابط:

http://www.qada.gov.ye/garymah.asp

(4) راجع: عبدا لله أحمد فروان، مرجع سابق، ص 48، وراجع ايضا: عبد المؤمن شجاع، جريمة التحويل الإلكتروني غير المشروع للأموال، مرجع سابق على الربط:

http://www.qada.gov.ye/garymah.asp

ب- الأموال المعلوماتية المعنوية

الأموال المعلوماتية المعنوية هي التي يثار الخلاف بشأن مدى خضوعها للقواعد العامة لجريمة السرقة، فهل يمكن إعمال الرأي الذي اعتمد على أن المعلومات لا يمكن تجريمها وفقا لنص السرقة ما لم تتضمنها دعائم مادية؟ معتبرا تجسد المعلومات في كيان مادي هو المبرر لتجريمها، وفقا لنص السرقة باعتبارها شيئاً مادياً ؟ أم تجريمها باعتبار أنها معلومات مستقلة بذاتها، سواء تم اختلاسها مع الدعامة المادية التي تحويها أم بدونها؟

فإذا ما اعتبرنا- وفقا للرأي الأول- أن المعلومات لا يمكن تجريم سرقتها مستقلة عن الوعاء المادي الذي يحويها، وأردنا تطبيق نص المادة (294)ع.ي، في حالة سرقة الدعامات التي تحوي المعلومات باعتبار أن المعلومات المعالجة مجسده في كيان مادي قابلة للتملك، ويمكن أخذها ونقلها وإدخالها في حيازة الجاني، حسب رأي بعض الفقهاء وأحكام القضاء، لوجدنا بالإضافة إلى أن هذا الرأي منتقد، فهو كذلك لا يتفق مع سياق نصوص القانون اليمني لمبررات هي:

1) يلاحظ بأن نص المادة (394) ع.ي، يحدد قيمة الشيء المسروق بما يعادل قيمة نصف جنية ذهب أبو ولد، وهي قيمة مرتفعة، مقارنة بالقيمة الضئيلة للدعامة، و يستحيل وفقا لذلك تطبيق نص المادة (394) وفقاً لهذا الرأي، كون السرقة – الحدية- في هذه الحالة قد فقدت أحد الشروط وهو عدم وصول قيمة المسروق إلى النصاب، بعكس المعلومات والبرامج التي تحويها الدعامة، والتي تقدر قيمتها بحسب أهميتها، وقد تصل إلى أكثر من القيمة المحددة للدعامة.

2) أن التجريم وفقا لذلك الرأي ينصب على الدعامة مع أن المستهدف من السرقة هو المعلومات، بسبب قيمة المعلومات المرتفعة، مقارنه بالقيمة الضئيلة للدعامة التي تحويها[1].

---

(1) ومن الأمثلة التي توضح قيمة المعلومات مقارنة بقيمة الدعامة قضية (HANCOCK.V. STATE) بالولايات المتحدة الأمريكية، وتتلخص وقائعها في قيام مبرمج في شركة تكساس للمعدات بنسخ 59 برنامجا مملوكا للشركة، والتقدم بعرض لبيعها لشركة منافسة مقابل 5 ملايين دولار، وفي دفاعه أمام المحكمة تمسك المتهم بأن قيمة البرامج التي نسخها لا تتعدى 35دولاراً، وهي قيمة الوعاء التي استخدمت لنسخها، وكان هدفه الاستفادة من قيمة المسروق الذي يحدده قانون العقوبات بولاية كاليفورنيا التي حدثت بها هذه الواقعة في جسامة السرقة وعقوبتها تبعا لقيمة الشيء المسروق، وفي فصل المحكمة فيما إذا كانت قيمة البرامج تستمد من استخداماتها ووظائفها أم من الأوراق التي استخدمت في نسخها، واستندت إلى تقرير الخبير بأن البرامج طبقا لما=

3) مع أن القانون اليمني قد تضمن عقوبات تعزيرية أخرى وفقاً لنصوص المواد(300، 301) - الحبس بما لا يتجاوز ثلاث سنوات، أو بما لا يقل عن ثلاث سنوات ولا يزيد عن عشر سنوات إذا صاحب السرقة بعض الأفعال مثل الإكراه أو التهديد بالسلاح- وذلك في حالة سقوط حد السرقة، والذي من مسقطاته ضآلة قيمة المال المسروق، إلا أن تطبيق تلك العقوبات – التعزيرية- قد يكون ممكنا في حالة ما إذا كانت قيمة المعلومات مع قيمة الكيان المادي ضئيلة، ولا يكون ذلك ممكنا في حالة ماذا كانت قيمة المعلومات كبيرة، تصل إلى النصاب المقرر لعقوبة جريمة السرقة الحدية مقارنة بالقيمة الضئيلة للدعامة لوجود نص آخر هو نص المادة (294) الذي يحدد نصاب المال المسروق في الجريمة الحدية، ونص المادة (298)الذي يحدد العقوبة، ويمكن تطبيقهما على هذه الحالة، وبالتالي فإننا سنتعامل بمعيارين لشيء هو في الأصل واحد وهو سرقة المعلومات، فنطبق نص المادة (300) التي تشمل عقوبة تعزيرية، إذا ما تم الاعتداء على المعلومات مع الدعامات التي تحويها عندما تكون قيمتها ضئيلة، ونطبق نص المادة (298) وهي العقوبة الحدية والأساسية لجريمة السرقة عندما تكون قيمة المعلومات مستقلة عن الدعامات كبيرة، فإذا ما عملنا ذلك نكون قد طبقنا عقوبتين مختلفتين على سرقة المستهدف فيها هو شيء واحد وهو المعلومات، سواء سرقة بذاتها أم بدعامتها.

وأمام المثالب التي تم إيضاحها والوصول إلى نتيجة، تتمثل في عدم إمكانية تطبيق نصوص السرقة في ق.ع.ي، وفقا للرأي القائل بعدم تحقق سرقة المعلومات إلا إذا اقترنت بالوعاء الذي يحويها، فإننا نرى إمكانية تطبيق نصوص السرقة في ق.ع.ي على سرقة المعلومات بذاتها، استنادا إلى مبررات الرأي الفقهي القائل بإمكانية تطبيق نصوص عقوبة السرقة على سرقة المعلومات مستقلة عن الدعامة التي تحويها، إضافة إلى المبررات التالية :

1) كون من يرون بأن المعلوماتية ليست مالا منقولا قد اعتمدوا على فهم القانون، وفقا لنصوص مواده التي تعتبر قديمة مقارنتا بالمعلوماتية وظهورها، فلم يكن المشرع

=تنتجه من إمكانات لمستخدمها تساوي 2.5 مليون دولار وبناء على ذلك، فلم تقبل المحكمة دفع المتهم، وعاقبته بعقوبة السرقة الأشد جسامة بالسجن 5 سنوات، معتمدة على قيمة البرامج وليس قيمة الأوراق المستخدمة في نسخها. راجع: آمل قارة الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص22 .

آنذاك مدركا لتلك الأموال وما ستؤل إليه، أما وقد أصبحت التعاملات المختلفة توضح قيمة تلك الأموال ألاقتصادية، بغض النظر عما إذا سلمنا أنها أموال مادية أو معنوية فلن يستطيع أحد أن ينكر القيمة ألاقتصادية لتلك الأموال وأهميتها في ذلك، فالسوق الإلكترونية المعاصرة عبر الإنترنت تعد أكبر سوق يتم عبرها تبادل العملة في المنتجات الاقتصادية اليومية، وكل ذلك بفضل تكنولوجيا المعلومات .

2) إضافة إلى أنه في حالة سرقة الكيانات المادية التي تحوي برامج أو معلومات، فإن المعلومات أو البرامج بلا شك وفي أغلب الأحوال هي المستهدفة من السرقة، وليست الكيانات المادية، وذلك بسبب القيمة الضئيلة للكيانات المادية، مقارنة بالمعلومات والبرامج، وهي بذلك تنتقل من حيازة مالكها إلى حيازة الجاني، بحكم إخضاعها لسيطرته.

3) أن المعلومات يمكن الاستئثار بها وحيازتها طالما تم نسخها، ومع أنه بالإمكان تطبيق قانون حماية حق المؤلف على عملية نسخ المعلومات والبرامج إذا توافرت شروط الاعتداء عليها وفقا لنصوص حقوق المؤلف، أما في حالة عدم توافر تلك الشروط فلامناص من تطبيق عقوبة السرقة، وإلا فإن تلك الجريمة ستظل بدون حماية جنائية.

4) لا يمكن التفرقة بين سرقة المعلومات عن طريق سرقة الوسائط المادية لها، و سرقة المعلومات بذاتها، لكون المعلومات هي المستهدفة من السرقة أولا وأخيراً، سواء تجسدت في صورة مادية بالدعامات، أم أنها قد تعرضت للنسخ وإعادة الإنتاج، ولأن القيمة الاقتصادية للمعلومات تفوق بكثير قيمة الدعامة، إضافة إلى ما تم إيضاحه بصدد نصوص قانون العقوبات اليمني المتعلقة بجريمة السرقة والتي لا يمكن تطبيقها على سرقة الدعامة، لعدم وصول قيمتها إلى القيمة التي تعتبر شرط لقيام جريمة السرقة، وبالتالي فإن تطبيق نصوص السرقة يكون تبعا للقيمة الاقتصادية للمعلومة، فتكون العقوبة وفقا لنص المادة (398) إذا بلغت قيمة المعلومة أو البرنامج النصاب، وتكون وفقا لنص المادة (300) ع.ي إذا لم تبلغ قيمة المعلومة نصاب السرقة.

وما تم ذكره من إخضاع المعلومات والبرامج المعالجة آليا لنصوص جريمة السرقة في القانون اليمني يقتصر على الصورة التي يقوم المتهم بالنسخ غير المشروع للبيانات المخزنة إلكترونيا، سواء كانت على هيئة نبضات كهربائية في دوائر إلكترونية مجمعة، أو على أشرطة واسطوانات ممغنطة .

أما الصور الأخرى التي تمت الإشارة إليها، والتي يمكن أن يتم بواسطتها الاستيلاء على المعلومات والبرامج المعالجة آليا، سواء عن طريق الالتقاط الهوائي للبيانات المعالجة والمنقولة إلكترونيا، أم الالتقاط الذهني عن طريق السمع والبصر، ففي هاتين الصورتين لا تتحقق جريمة السرقة وفق نصوص القانون اليمني، ويمكن تبرير ذلك بالآتي:

1) كون نص المادة 294ع.ي في تحديده للفعل الذي ترتكب به الجريمة استعمل لفظ (أخذ) ولم يستعمل لفظاً يدل على الالتقاط، ولفظ الأخذ يتناسب مع الأشياء المادية المحسوسة، ويمكن أن يتناسب اللفظ مع أخذ المعلومات من أماكن وأدوات تخزينها، أما الالتقاط فهي تدل على الاستيلاء على موجات طليقة في الهواء، بالتقاط الإشعاعات الكهرومغناطيسية أثناء انبعاثها أو نقلها.
2) وإذا كان بالإمكان تجريم الصورة الأولى في حالة نص القانون عليها صراحة إذا تم تعديله ، فلا يمكن تجريمها في الحالة الثانية التي تتعلق بالالتقاط الذهني للمعلومات، على أساس أن التجريم في مثل هذه الحالة لا يتطابق مع المنطق، وإلا أصبح وفقا لهذا المفهوم الحق في تجريم ما يدور بالعقول والأذهان، وقد سبق إيضاح ذلك في موضعه.

أخيرا وإزالة للالتباس والاختلاف الوارد بهذا الشأن فإن على المشرع اليمني الإسراع في إصدار قانون لمواجهة الجرائم المعلوماتية، على أن يضمنه نصا خاصا بجريمة السرقة المعلوماتية، أو يضمن قانون العقوبات تعديلا لنصوص جريمة السرقة، يوضح من خلالها طبيعة المال المعلوماتي وإدراجه ضمن الأموال القابلة للسرقة، وكذلك الأفعال التي يمكن أن يتم ارتكاب تلك الجريمة بواسطتها كالتقاط المعلومات أثناء تشغيل الجهاز، أو أثناء تبادل المعلومات وانتقالها من جهاز إلى آخر أو يضيف عبارة بأي وسيلة أو بأي طريقة كانت .

أما المشرع الجزائري فقد أصدر القانون رقم(04 – 15) المؤرخ في 10 نوفمبر 2004 بخصوص المساس بأنظمة المعالجة الآلية للمعطيات، وكذلك القانون رقم (09-04) الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، وذلك في حد ذاته يعد ميزة لمواجهة ذلك النوع الحديث من الإجرام، إلا أن القانون الأول قد خلا من النص على تجريم سرقة المعلومات، كما أن الثاني أورد نصا عاما يدخل الجرائم التقليدية في إطار التجريم وفقا لقانون العقوبات النافذ ولم يتضمن نصا خاصا بهذه الجريمة، وإزالة للالتباس والخلاف الوارد بشأنها في مجال الفقه القانوني أو القضاء، فلا مناص من الرجوع لقانون العقوبات لمعرفة موقفه من تلك الجريمة، بالاستعانة بما تم إيضاحه من آراء الفقه وبعض أحكام القضاء الفرنسي في هذه المسألة.

ولمعرفة موقف قانون العقوبات الجزائري حيال سرقة المعلومات وهل بالإمكان تطبيق نص المادة (350) ع.ج فسوف يتم إيضاح محل الجريمة والركن المادي لها لبيان مدى تطابقهما مع المحل والركن المادي في حالة سرقة المعلومات.

فمن حيث محل جريمة السرقة وكما سبق الإيضاح فإنه يتطلب أن يكون المسروق محل الجريمة مالاً منقولاً مملوكاً للغير. وعند مطالعة قانون العقوبات الجزائري يلاحظ بأنه لم ينص بصورة صريحة على لفظ المال، أو أن يكون ذلك المال منقولاً كما فعل المشرع اليمني[1]، حيث استبدل المشرع الجزائري لفظ المال بلفظ الشيء، وفقا لنص المادة (350) ع،ج بالنص على (كل من اختلس شيئا غير مملوك له يعد سارقا)، ولفظ الشيء في نص المادة يوحي بأن النص من حيث الأساس يخص الأموال المادية، ويجب أن يكون المال المسروق منقولا، ولو أن هذا الشرط لم يرد صراحة في النص القانوني[2] .

ويلاحظ من خلال ظاهر النص القانوني أنه أخذ بالمفهوم المادي لمحل السرقة، وذلك يقودنا إلى نتيجة مفادها استبعاد المعلومات من مجال تطبيق السرقة عليها.

ويؤيد هذه النتيجة جانب من الفقه الفرنسي سبق الإشارة إليه، إلا أن الفقه الحديث والقضاء في فرنسا قد خالف ذلك الاتجاه، واعتبر المعلومات محلا للسرقة، حيث خلص

(1) راجع المادة (294) من قانون الجرائم والعقوبات، والمادة (350)من قانون العقوبات الجزائري.
(2) أحسن بوسقيعه، الوجيز في القانون الجزائي الخاص، ج1، ط5، دار هومه، الجزائر، 2006، ص 256.

إلى أن المعطيات المعلوماتية صالحة لأن تكون محلا للسرقة، ويتحقق ذلك بتحويل ما يحتويه قرص من معلومات إلى سند آخر حتى لو كان الاختلاس مؤقتا ولم يدم إلى الوقت اللازم لنقل ما يحتويه القرص إلى ذلك المستند(1)، ويمكن إعمال ذلك وتطبيقه في الجزائر، نظرا لتطابق التشريعين بشأن هذه المسالة(2)، فقد ذكر المشرع الجزائري وكذا الفرنسي لكلمة شيء(3) تعبيرا عن المال المنقول، وجاء الفظ في كلا التشريعين مطلقا دون قيد ودون وصف لأن يكون الشيء ماديا أو معنويا، وذلك يقتضي بأن اللفظ يشمل الأشياء المادية والمعنوية، وكل شيء قابل لأن يكون محلا للسرقة، كما يشترط أن يكون للشيء قيمة، سواء كانت القيمة مادية أو تجارية أو حتى أدبية كالخطابات المهمة وطوابع البريد المستعملة، إلا أنه لا يشترط أن تكون القيمة كبيرة فقد تكون ضئيلة.

ولكون الأشياء المعنوية قد زادت قيمتها الاقتصادية بزيادة تدفقها وأهميتها، حيث إن بعضها يفوق في القيمة بعض الأموال المادية منقولة كانت أو عقارية، فإن ذلك يؤكد الطبيعة المالية للمعلومات.

ومع أن المشرع الجزائري لم يكن في ذهنه تلك الأشياء المعنوية وقت وضعه للنص فإن ذلك لا يحول دون إمكانية وقوع السرقة على شيء معنوي.

إضافة إلى أن عدم تحديد طبيعة الشيء محل السرقة هو الذي دفع إلى القول بإمكانية اختلاس التيار الكهربائي على الرغم من أنه ليست له طبيعة ماديه، ومبدأ تجريم الاستيلاء على الطاقة يطبق على كل قوة أو طاقة يمكن إخضاعها لسيطرة الإنسان، ويكون بوسعه أن يوجهها على النحو الذي يحقق منفعته، وبرامج ومعلومات الحاسوب يصدق عليها هذا المعنى، وتقبل التملك والحيازة من خلال الدعامة التي توجد عليها، ولا تنقل إلا بموافقة حائزها بعد معرفة كلمة السر، وهي على هذا النحو وعلى الرغم من

---

(1) تطور القضاء الفرنسي باتجاه الإقرار بسرقة المعلومات ، وبهذا الخصوص فقد صدر قرار حديث في فرنسا عن محكمة الاستئناف بليموج الفرنسية (Limoges)، بتاريخ 1998/9/8 م في قضيه تتمثل وقائعها في كون أجير استدل في دعوى أمام المحكمة العمالية بوثائق اختلسها من مستخدمه، وعوضا من أن يستنسخها، قام بنقل مقاطع منها باليد، توبع هذا الأجير من أجل السرقة وأدين على أساس انه أرتكب جريمة السرقة، وجاء في مسببات الحكم بأن العامل في مؤسسة والذي تكون في حيازته الملدية وثائق تابعة لرب العمل وينقل جزءاً منها، لأغراض شخصية، دون علم وبغير رضا صاحبها للاستدلال بها أمام القضاء يكون مقترفا لجريمة السرقة. لمزيد من التفصيل راجع: أحسن بو سقيعه، الوجيز في القانون الجزائي الخاص، مرجع سابق، من ص259 إلى ص261.

(2) أحسن بو سقيعه، المرجع السابق، ص256.

(3) انظر المادة (379) من ق.ع.ف قديم المعدلة بالمادة (2/311) ق.ع .ف جديد ويقابلها نص المادة (350) من ق.ع.ج.

أنها شيء غير مادي فإنها تصلح محلا لجريمة السرقة، ولا يمثل ذلك خروجا على مبدأ الشرعية، كون نصوص جريمة السرقة تقبل هذا التفسير، لكونها لم تحدد طبيعة الشيء ماديا أو معنويا ولكون الأشياء المعنوية يصدق عليها وصف المال، نظرا لقيمتها الاقتصاديه[1].

والخلاصة، فإن المشرع الجزائري بهذا النهج قد حذا حذو المشرع الفرنسي ابتداء من النص، على أن محل الاختلاس في جريمة السرقة الشيء، وكما ذكرنا سابقا للفقهاء الفرنسيين الذين اعتبروا المعلوماتية مالا منقولا تخضع للقواعد العامة في جريمة السرقة، وفقا لقانون العقوبات الفرنسي الذي أورد في نص المادة(379 .ع ف قديم المعدلة بالمادة 2/311 ع.ف جديد) لفظ "الشيء" وفسرها بعض الفقهاء إضافة إلى اتجاه القضاء الحديث بأنها تشمل الأشياء المادية والأشياء المعنوية، واعتبروها تشمل الأموال، وتكون مملوكه للغير، كونها قابله للاستئثار والحيازة، وبالتالي فإنه يمكن نقلها وحيازتها. وبناء عليه فيمكن القول بأن جريمة سرقة المعلومات والبرامج المعالجة آليا تخضع لنص المادة(350) ع.ج، ويؤكد ذلك الرأي بعض الفقهاء في الجزائر[2].

ونرى بعد هذا الإيضاح بأن على المشرع الجزائري طالما وكان له السبق في التشريعات العربية التي تناولت تجريم الاعتداء أو المساس بأنظمة المعالجة الآلية للبيانات، وغيرها من الجرائم التي يمكن أن ترتكب أو يسهل ارتكابها بواسطة نظم المعلوماتية، أن يعمل على تلاشي القصور في التعديلات القادمة للقانون، ويضيف النصوص القانونية التي تجرم الأفعال التي لم يتم النص عليها، ومن ذلك اعتراض المعلومات، أو التقاطها، وتحديد طبيعة المال محل السرقة، وكذلك جريمة التزوير في مجال المعلوماتية، وغير ذلك من أوجه القصور التي يرتئيها فقهاء القانون في الجامعات الجزائرية، فلا زال القصور يكتنف أغلب التشريعات في هذا المجال بما فيها التشريعات الحديثة، لذلك يتم تعديلها بين وقت وآخر ومن تلك التشريعات التشريع الفرنسي، الذي تم تعديله ثلاث مرات كان آخرها في 2004.

---

(1) آمل قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص28، وص29.

(2)أحسن بو سقيعه، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص259 وما بعدها. وراجع أيضا: آمل قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص28،وص29.

المطلب الثاني

جريمة النصب (cheating crime)

لم يعرف المشرع اليمني وكذلك الجزائري جريمة النصب واكتفيا بتحديد النموذج القانوني لها والذي من خلاله يمكن تحديد أركانها ووسائل ارتكابها.

وبالعودة إلى التعريفات الفقهية للجريمة فيمكن تعريفها بأنها: (الاستيلاء على منقول مملوك للغير بخداع المجني عليه وحمله على تسليمه)[1].

كما عرفها البعض بأنها : (الاستيلاء على الحيازة الكاملة لمال الغير، بوسيلة يشوبها الخداع وتسفر عن تسليم ذلك المال) [2].

والنصب في مجال المعلوماتية يقتضي إدخال المعطيات أو تغيير البرنامج للحصول على المنقول أو الأموال بالاستعانة بالطرق الاحتيالية[3].

كما عرفت هيئة الأمم المتحدة الاحتيال المعلوماتي بناء على التوجيه رقم(Rg 89/) المتبنى من المجلس الأوربي بأنه: (الإدخال[4] أو المحو أو التعديل أو كبت البيانات وبرامج الحاسوب، أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية، أو فقد حيازة ملكية شخص، بقصد الحصول على مكسب اقتصادي غير مشروع له أو لشخص آخر"[5].

و لم يتضمن قانون العقوبات اليمني وكذلك الجزائري نصوصاً قانونية صريحة تجرم النصب في مجال المعلوماتية، وإذا كان الأمر يبدو مقبولا في القانون اليمني، لعدم صدور نصوص قانونية للجرائم المعلوماتية بشكل عام، ومنها جريمة النصب، فقد لا يبدو كذلك بالنسبة للقانون الجزائري نظرا لتضمين قانون العقوبات نصوصاً تتعلق

---

(1) محمود نجيب حسني، الجرائم المضرة بالمصلحة العامة وجرائم الاعتداء على الأشخاص، دار النهضة العربية، القاهرة، 1986، ص990، مشار إليه لدى حسن علي مجلي، جرائم الاعتداء على الملكية في القانون والقضاء اليمني، ط1، عالم الكتب اليمنية، صنعاء، 2007م، ص111.

(2)هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ص 286.

(3) نصرون ورديه، جرائم الغش في الإعلام الآلي، مطبوعة مقررة على طلبة المعهد العالي للقضاء بالجزائر، ص9.

(4) ومن القضايا التي حدثت في مجال التلاعب بالبيانات عام 1994 قيام احد مدخلي البيانات العاملين في إحدى الشركات المساهمة في الأردن من تسجيل (78300)سهم بأسماء شركاء وهميين وإخراج شهادات بملكية الأسهم لمالكيها ومن ثم القيام ببيعها في السوق المالية بمبلغ مائة وتسعين ألف دينار أردني .راجع: أحمد الكركي :جريمة التلاعب في بيانات الحاسوب، بحث مقدم إلى أكاديمية الشرطة الملكية بعمان ، 1996، ص29، مشار إليه لدى محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، مرجع سابق، ص56.

(5) محمود أحمد عباينة، المرجع السابق، ص 54، وص55.

بالمساس بأنظمة المعالجة الآلية للمعطيات دون أن تشمل جريمة النصب في مجال المعلوماتية[1]، ومع أن القانون رقم (09- 04) المؤرخ في 5 غشت(أغسطس) الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما قد تضمن تجريم الجرائم التقليدية التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، إلا أن النص قد ورد عاما يشمل جميع الجرائم التقليدية، ولا يخص جريمة بعينها.

وبناء على ذلك سيتم إيضاح أركان الجريمة وفيما إذا كانت النصوص الحالية في قانوني العقوبات اليمني والجزائري تنطبق على جريمة النصب في مجال المعلوماتية من خلال المقارنة بين القواعد العامة للجريمة والقواعد الخاصة في مجال المعلوماتية .

1- الركن الشرعي ومحل جريمة النصب

أ- الركن الشرعي لجريمة النصب

تضمنت العديد من المواد في ق.ع.ي، وق.ع.ج تجريم جريمة النصب، وقد استخدم القانون اليمني لفظ النصب بينما استعمل القانون الجزائري لفظ الإحتيال، وكلاهما يرميان في نهاية الأمر إلى معنى واحد وهو الخداع.

حيث نصت المادة (310)ع.ي يمني على أن (يعاقب بالحبس مدة لاتزيد على ثلاث سنوات، وبالغرامة من توصل بغير حق إلى الحصول على فائدة مادية لنفسه أو لغيره، وذلك بالاستعانة بطرق احتيالية (نصب) أو اتخذ اسماً كاذباً أو صفة غير صحيحة).

كما نصت المادة(372) ع.ج على أن: (كل من توصل إلى استلام، أو تلقي أموال، أو منقولات، أو سندات، أو تصرفات، أو أوراق مالية، أو وعود، أو مخالصات، أو

(1) جرم القانون رقم (04-15) المؤرخ في 10نوفمبر 2004 المساس بأنظمة المعالجة الآلية للمعطيات، ولم يشر إلى جريمة النصب والسرقة والتزوير في مجال المعلوماتية، وقد نجد مبررا لذلك من خلال العنوان الذي وضعة المشرع الجزائري لتلك الجرائم والذي من خلال ألفاظه يتضح بأنه قد أتى خصيصا لتجريم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، أما عندما ترتكب جرائم بواسطة الأنظمة وتستهدف المعلومات بهدف تحقيق نتيجة معينة فقد تكون تلك الجرائم في نظر المشرع الجزائري موجودة أصلا والفارق بالنسبة للأخيرة هو ارتكابها بوسائل إلكترونية، وبالتالي يمكن إخضاعها لقانون العقوبات في نصوصه التقليدية أو لقوانين أخرى ذات صلة بالجريمة، إلا أنه من ناحية أخرى إذا تعدينا موضوع العنوان لذلك القسم من الجرائم فسنجد بعض المواد قد جرمت الاعتداء على المعطيات بحد ذاتها، سواء تمثل ذلك بإدخالها إلى النظام عن طريق الغش أو تعديلها أو إزالتها كما في نص المادة (394 مكرر 1)،و(394مكرر2)، مما يدل على أن المشرع الجزائري قد أخطأ في صياغة العنوان، وكان يفترض أن يكون العنوان هو "المساس بأنظمة المعالجة الآلية للمعطيات والبيانات والبرامج المعالجة آليا".

إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه، إما باستعمال أسماء أوصفات كاذبة، أو سلطة خيالية، أو اعتماد مالي خيالي، أو بإحداث الأمل في الفوز بأي شيء، أو في وقوع حادث، أو أية واقعة أخرى وهمية، أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 دج إلى 20.000 دج.

وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو إذونات أو حصص أو أية سندات مالية، سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات، والغرامة إلى 20.000دينار)[1].

ومن خلا النصين اليمني والجزائري يلاحظ بأنهما قد وضحا الأركان المكونة للجريمة ووسائل ارتكابها، وقد اتسم النص اليمني بالعموم، سواءٌ من حيث تحديد الأموال محل النصب، أم من حيث الوسائل التي يتم ارتكاب النصب بواسطتها، فاقتصر على توضيح الأموال بالفائدة المادية للجاني أو لغيره، لكي يترك المجال واسعا أمام القضاء في تجريم كل ما يجلب الفائدة للجاني أو لغيره، وبالنسبة لوسائل الاحتيال فقد اكتفى المشرع اليمني في تحقق جريمة النصب في اتخاذ الجاني اسمً كاذبًا أو صفة غير صحيحة أو الاستعانة بالطرق الاحتيالية دون أن يوضح الطرق الاحتيالية أو يذكر لذلك أمثلة، كما فعل المشرع الجزائري، حيث أوضح الطرق التي يستعان بها لتحقيق جريمة النصب، كما أنه أوضح عن ماهية الأموال التي تكون محلا لجريمة النصب بصورة أدق من القانون اليمني.

ومن خلال النصوص القانونية وتعريف الفقه لجريمة النصب يتضح بأنها تختلف عن جريمة السرقة، فالمال في السرقة يتم انتزاعه وتحويل حيازته بدون رضا المجني عليه، بمعنى آخر فإن الجاني يقوم بأخذ المال على المجني عليه، بعكس النصب فإن

---

(1)ويلاحظ البعض بأن النص بالعربية قد ورد مبتوراً ولا يؤدي المعنى المتوخى منه حسب ما يتبين من النص في نسخته الفرنسية، وأن الصياغة السليمة كما نصت المادة(372) ق.ع ج بالفرنسية وهي: (كل من توصل إلى استلام أو تلقي أموالا أو منقولات أو سندات أو تصرفات أو أوراقا مالية أو وعودا أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه، إما باستعمال أسماء أوصفات كاذبة وإما باستعمال مناورات احتيالية لإيهام الغير بوجود سلطة خيالية أو اعتماد مالي خيالي، أو لإحداث الأمل في الفوز بأي شيء أو الخشية من وقوع حادث أو أية واقعة أخرى وهمية، يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000دينار) راجع: أحسن بو سقيعه، الوجيز في القانون الجزائي الخاص، مرجع سابق، ص256.

المجني عليههو من يقوم بتسليم المال للجاني متأثراً بالأمور الاحتيالية التي اتخذها الجاني للتدليس على صاحب المال.

فهل بالإمكان تطبيق تلك النصوص على الجريمة في مجال المعلوماتية ؟ ذلك ما سيتم توضيحه من خلال بيان باقي أركان الجريمة.

ب- : محل جريمة النصب

1) محل جريمة النصب وفق القواعد العامة

محل جريمة النصب هو نفس محل جريمة السرقة وهو المال المنقول المملوك للغير .

يجبأن يكون محل الجريمة مالاً ، بحيث لا يسال من يتوصل بأي وسيلة احتيالية إلى أي شيء آخر غير المال، و يكون ذا قيمة مثله مثل المال المسروق، والخلاف يكمن في قيمة المال في السرقة، وفقا للقانون اليمني، حيث يتطلب أن تكون للمال قيمة معينة، أما في النصب فلم يشترط القانون أن يكون للمال محل النصب قيمة كبيرة، بل إن الجريمة تقع بغض النظر عن أن تكون قيمة المال كثيرة أم قليلة.

كما يشترط في المال أن يكون ذا طبيعة مادية، فلا يعد نصبا استعانة المتهم بوسائل احتيالية في سبيل الحصول بغير حق على منفعة غير مادية، حتى لو كانت للمنفعة قيمة مالية، وبناء على ذلك فلا يعد نصبا من يتوصل بطريقة احتيالية على حمل البائع على تقسيط ثمن الشيء المبيع حتى لو عجز عن دفع الأقساط، لكونه لم يقصد سلب مال المجني عليه (1).

والأشياء ذات القيمة الأدبية تصلح لأن تكون محلا لجريمة النصب، لكونها تقوم بالمال وتعتبر جزءاً من الذمة المالية لصاحبها ومن ثم تدخل في تكوين ثروته، فالمذكرات والخطابات والتذاكر يمكن أن تصل أثمانها إلى مبالغ كبيرة(2).

ويشترط : أن يكون المال محل الجريمة مالا منقولا، ومع أن القانون اليمني لم ينص على ذلك بصورة صريحة مثل القانون الجزائري في المادة (372) التي ضمنت المنقولات ضمن الأشياء التي تقع عليها جريمة النصب، إلا أن ذلك الشرط يمكن استخلاصه من نص المادة (310) من ق.ع يمني والتي تنص على عقاب من توصل

---

(1) حسني الجندي ، ومجدي عقلان، شرح قانون العقوبات اليمني، مرجع سابق، ص238.
(2) حسني الجندي، ومجدي عقلان، المرجع السابق، ص 238، وص139.

بغير حق إلى الحصول على فائدة مادية بالطرق الاحتيالية، فالفائدة المادية تدل على أن المال محل النصب منقول وبالتالي فلا تقع الجريمة على العقارات بطريقة مباشرة وإنما تقع بطريقة غير مباشرة، إذا ما تم الاستيلاء على عقد البيع أو رهنه.

كما يشترط أن يكون المال مملوكا للغير، فلا تقع الجريمة على الأموال التي يمتلكها المحتال، ومنها على سبيل المثال الأموال التي آلت إلى الشخص عن طريق الميراث، وقام بالاستيلاء عليها عن طريق الاحتيال وهو لا يعرف، وقد سبق أن تم إيضاح أنالبرامج والمعلومات تعد أموالاً مملوكة لصاحبها، من خلال استئثاره بها والتصرف فيها كغيرها من الأموال، ولكونها تشكل قيمة اقتصادية، ويكتفى بما تمت الإشارة إليه بهذا الخصوص في جريمة السرقة في مجال المعلوماتية.

2) محل جريمة النصب في مجال المعلوماتية

يتمثل محل جريمة النصب في مجال المعلوماتية بالمكونات المادية والبرامج والبيانات المخزنة في دعامات، وكذلك البيانات والبرامج المعالجة آليا، حيث تعد الأخيرة هي الأهم، والتي سيتم التركيز عليها في مجال الدراسة، نظرا للخلاف الكائن حول صلاحيتها لأن تكون محلا لجريمة النصب[(1)]. بعكس المكونات المادية والبرامج والبيانات المخزنة في دعائم والتي لا تثير مشكلة في صلاحيتها لأن تكون محلا لجريمة النصب عند أغلب الفقهاء باعتبارها أموالاً ذات طبيعة مادية [(2)].

و حول صلاحية البرامج والبيانات المعالجة آليا لأن تكون محلا لجريمة النصب إذا كانت في صورة مستقلة عن الدعامة المادية فقد وجد خلاف في الرأي بهذا الشأن.

- عدم صلاحية البرامج والبيانات لان تكون محلا لجريمة النصب، وذلك لعدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام في جريمة النصب، وحتى في حالة الافتراض من أن التسليم والاستلام قد تم فإنه لا يترتب على ذلك حرمان مالك البيانات أو البرنامج من حيازتها، كونها تبقى تحت سيطرته التامة[(3)].

(1) فيتم التلاعب بالبرامج والبيانات بهدف تحويل كل أو بعض أرصدة الغير، أو الفوائد المستحقة لهم إلى حساب الجاني أو عن طريق التلاعب في الإشارات الإلكترونية المرتدة من الحاسوب المركزي إلى جهاز الصراف الآلي للنقود لاختلاس أموال من أرصدة العملاء أو من رصيد جهاز الصراف نفسه، دون التأشير في بيانات الحاسوب المركزي أو في حسابات العملاء. لمزيد من التفصيل راجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 270.

(2) عفيفي كامل عفيفي، مرجع سابق، ص146.

(3) علي عبد القادر القهوجي، مرجع سابق، ص58.

كما أنه يستلزم في جريمة النصب أن يكون الجاني قد خدع إنسالاً مثله، وأن يكون الإنسان المخدوع مكلفا بمراقبة البيانات[1]. ولكون المعلومات والبرامجليس لأيٍ منهما قوام مادي مستقل بذاته، فلا يتحقق لهما صفة المال، وبالتالي فليس هناك ما يمنع من التدخل التشريعي لتجريم الاعتداء على هذه المكونات غير المادية[2].

- صلاحية البرامج والبيانات المعالجة آليا لأن تكون محلا لجريمة النصب، ويؤيد هذا الرأي جانب من الفقه الفرنسي باعتبار أن خداع النظام المعلوماتي بهدف سلب مال الغير، تتحقق به الطرق الاحتيالية ككذب تدعمه أعمال مادية أو وقائع خارجية، وهي إبراز المستندات المعلوماتية التي تدخل النظام المعلوماتي، كما تتحقق طرق النصب باستخدام الجاني المستندات غير الصحيحة التي يخرجها الحاسوب، بناء على ما وقع في برامجه أو في البيانات المخزنة بداخله من تلاعب، كي يتم الاستيلاء على أموال لاحق له فيها [3].

2- الركن المادي لجريمة النصب

لبيان الركن المادي لجريمة النصب في مجال المعلوماتية لابد من إيضاح الركن المادي لجريمة النصب وفقا للقواعد العامة

أ- الركن المادي في جريمة النصب وفقاً للقواعد العامة

الركن المادي في جريمة النصب وفقاً للقواعد العامة في أغلب القوانين ومنها القانون اليمني والقانون الجزائري، يتمثل باستعمال المناورات والطرق الاحتيالية، وهو الكذب البالغ درجة الاحتيال الذي ينتج عنهتسليم المجني علية مالاً من أمواله إلى الجاني[4].

فالعنصر الأول في الركن المادي يتمثل من خلال قيام الجاني باستخدام إحدى الطرق الاحتيالية التي من شأنها إيهام المجني عليه وجعله لا يدرك حقيقة تلك الأفعال، وبالتالي يقدم على تسليم الشيء الذي يهدف الجاني إلى تسلمه، ولابد لاكتمال الركن

(1) Martine Briat , la délinquance informatique, Aspects de droit comparé In la droit criminel face aux technologies nouvelles de la communications , Economisa 1986 ,p.266

مشار إليه لدى أحمد خليفة الملط، مرجع سابق، ص 400 وهذا الرأي يمثل وجهة نظر بعض الفقهاء في فرنسا.

(2) عمر الفاروق الحسيني، مرجع سابق، ص339.

(3) راجع هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مرجع سابق، ص 274.

(4) حسن علي مجلي، جرائم الاعتداء على الملكية في القانون والقضاء اليمني، ط1، عالم الكتب اليمنية، صنعاء،2007، ص166.

المادي في جريمة النصب وجود علاقة سببية بين فعل الاحتيال والنتيجة المترتبة عليه والمتمثلة بتسلم المال محل الجريمة.

وإذا كانت الطرق الاحتيالية أو وسائل التدليس قد وردت على سبيل الحصر في ق.ع.ج[1]، فإن تلك الطرق والوسائل لم تأت على سبيل الحصر في ق. ع.ي، بحيث اقتصر نص المادة (310) على الإشارة إلى ارتكاب تلك الجريمة بالاستعانة بطرق احتيالية، أو اتخاذ اسم كاذب أو صفة غير صحيحة دون ذكر تلك الطرق، وقد يكون ذلك لكثرة تلك الوسائل والأساليب التي يتم بواسطتها الاحتيال وعدم حصرها في وسائل معينة. وقد اكتفى المشرع اليمني بتحديد تلك الطرق ببيان نوعها والغرض منها، فمن حيث النوع يجب أن تكون تلك الطرق والوسائل ذات مظهر خارجي يستغلها الجاني لدعم كذبه والظهور بمظهر الحقيقة، ومن حيث الغرض ينبغي أن تكون غاية الجاني من استعمال تلك الطرق والوسائل أخذ مال الغير [2].

فالسلوك المادي المكون للطرق الاحتيالية في جريمة النصب يتمثل بأي فعل يقوم على الكذب، ويدعم بمظاهر خارجية من شأنها أن تجعل ذلك الكذب بمثابة وقائع صحيحة وحقيقية .

ومن المظاهر الخارجية التي تدعم الكذب وتجعله يبلغ مبلغ الطرق الاحتيالية:

- الاستعانة بالغير.
- الاستعانة بأوراق غير صحيحة.
- القيام ببعض الأعمال المادية
- استغلال الصفة أو الثقة.

(1) حددت المادة(372) من الأمر رقم (66- 156) المؤرخ في8 يونيو 1966 يتضمن قانون العقوبات الجزائري المعدل والمتمم، الطرق والوسائل التي تستخدم في ارتكاب جريمة النصب إما باستعمال أسماء أوصفات كاذبة، وإما باستعمال مناورات احتيالية لإيهام الغير بوجود سلطة خيالية أو اعتماد مالي خيالي أو لإحداث الأمل في الفوز بأي شيء أو الخشية من وقوع حادث أو أية واقعة أخرى وهمية، فوسائل التدليس تكمن في آمرين :أ- استعمال أسماء وصفات كاذبة 2- استعمال المناورات الاحتيالية : وتتمثل بكذب مصحوب بوقائع ومظاهر خارجية لإيهام المجني عليه وجعله يدرك الأمر على غير حقيقته، كأن يستعين الجاني بأشياء يرتبها بطريقة معينة، بحيث تصبح دليلا على صدق ما يدعيه يتم من خلالها الاحتيال على المجني عليه، ومنها الاستعانة بشخص آخر لتأكيد وتدعيم أقوال النصاب ويكون الغرض من استعمال الطرق الاحتيالية إيهام الغير بوجود سلطة خيالية أو اعتماد مالي خيالي أو لإحداث الأمل في الفوز بأي شيء أو الخشية من وقوع حادث أو أية واقعة أخرى وهمية . لمزيد من الإيضاح راجع: أحسن أبو سقيعة، مرجع سابق، ص313.

(2)حسني الجندي، شرح قانون العقوبات اليمني، مرجع سابق، ص248.

ويشترط في تدخل الغير أن يكون للغير قدر من الاستقلالية بموجب اتفاق مسبق مع الجاني، يكون سبباً في إقدام المجني عليه بتسليم أمواله للجاني، ومثال ذلك قيام شخص بزيادة قيمة السلعة أثناء محاولة مشتر شراءها لإيهام المجني بأن السلعة تستحق أكثر من ذلك.

كما يشترط في الأوراق المقدمة إلى المجني عليه أن تكون غير صحيحة، وأن تكون منسوبة إلى الغير، سواء كان هذا الغير حقيقيا أم وهميا .

أما الإعمال المادية فهي كثيرة وغير قابلة للحصر وبالتالي فقد تتمثل بالظهور بمظهر الغنى أو الثراء أو غير ذلك من الأفعال التي توهم المجني عليه فتجعله يقدم على تسليم أمواله.

كما أن استغلال الصفة أو الثقة من شأنها أن تكون من ضمن المظاهر الخارجية التي تدعم الكذب وتحقق ارتكاب جريمة النصب، والصفة أو الثقة لابد أن تكون حقيقية ومعروفة لدى الآخرين .

وكما أن المظاهر الخارجية تعد شرطا لارتكاب جريمة النصب في حالة الكذب البالغ مبلغ الطرق الاحتيالية، فهي لا تعد شرطا أو يمكن الاستغناء عنها في حالة اتخاذ اسم أو صفة كاذبة، بمعنى آخر فإن قيام الجاني باتخاذ اسم كاذب أو صفة كاذبة بهدف الاستيلاء على منفعة أو مال للمجني عليه أو للغير، يتحقق بهما جريمة النصب إذا توافرت باقي الأركان.

واتخاذ الاسم الكاذب هو اتخاذ الجاني أو ادعاؤه باسم كاذب يحمل شهرة، كاسم العائلة أو حتى الاسم الأول، سواء كان الاسم حقيقيا أم وهميا، المهم فيه هو أنه يحمل شهرة، وعلى العكس من ذلك لا يعد اسم الشهرة أو الاسم الذي يدعى به الشخص من الأسماء الكاذبة .

والصفة غير الصحيحة تتمثل في قيام المتهم بادعاء مركز معين أو وظيفة معينة كادعائه بأنه حاصل على شهادة الدكتوراه أو أنه يحمل رتبة لواء أو أنه يعمل طبيبا أو محاميا.

ويجب عدم الخلط بين استعمال صفة غير صحيحة واستعمال صفة حقيقية، فالأولى تقوم بها الجريمة مستقلة، أما الثانية فلا بد لها من مظاهر مادية تؤكد ذلك .

ولابد لقيام الجريمة أن يكون سلوك المتهم - سواء تمثل بادعاءات كاذبة تدعمها مظاهر خارجية أم اتخاذ اسم كاذب أو صفة غير صحيحة - بهدف الحصول على فائدة مادية أو التوصل إلى مال الغير، ويمكن تحقيق تلك الغاية بعدة صور أشارت إليها معظم القوانين ومنها القانون الجزائري ومن تلك الصور، الإيهام بوجود مشروع كاذب، أو واقعة مزورة، أو الإيهام بوجود سند دين غير صحيح، أو الإيهام بوجود سند مخالصة مزور، أو الإيهام باحتمال وجود الشيء في المستقبل، مثل إحداث الأمل بحصول ربح وهمي، أو إحداث الأمل بتسديد المبلغ الذي أخذ بطريق الاحتيال، وجميع هذه الغايات تحمل المجني عليه إلى الاعتقاد الكاذب بوجود شيء واقع أو احتمال وجوده مستقبلا، ويلاحظ بأن القوانين ومنها القانون الجزائري قد استعملت عبارات عامة للنص على حماية الغير من المناورات الهادفة إلى إقامة أو إزالة روابط قانونية، حيث ذهب القضاء الجزائري إلى تأويل واسع لتلك العبارات، لتشمل كل تصرف يكون الغرض منه إيهام الدائن خطأ بأنه قد استلم حقه (1).

أما العنصر الثاني قي الركن المادي لجريمة النصب فيتمثل في الاستيلاء على مال مملوك للغير، ويكون ذلك بتسليم المجني عليه لذلك المال إلى الجاني، بناء على الوسائل الاحتيالية التي وقعت عليه، فإذا تحقق التسليم فإن الجريمة تصبح تامة (2).

والتسليم سلوك يصدر من المجني عليه بسبب الاحتيال عليه من جانب الجاني الذي يحمله على القيام بتصرف مالي من شأنه نقل المال موضوع الجريمة إلى الجاني، أو أي شخص آخر بعينه.

ويشترط في التسليم أن تكون إرادة المجني عليه وقت التسليم معيبة، وذلك ما يميز جريمة النصب عن جريمة السرقة التي يشترط في التسليم أن لا يكون إراديا، حيث إن التسليم الإرادي الصادر عن إرادة حرة ومدركة ينفي الاختلاس في السرقة، حتى لو كان ناتجا عن الغش أو الغلط، بعكس التسليم في النصب الذي يشترط في التسليم أن يكون ناتجا عن إرادة معيبة.

فإذا ما تحقق التسليم الناتج عن الإرادة المعيبة فإن الواقعة تتحقق، بغض النظر عما إذا كان التسليم يدويا أو حكميا، أما إذا قام الجاني باستغلال ظروف معينة في الاستيلاء

(1) أحسن ابو سقيعة ، مرجع سابق، ص314.
(2) حسن علي مجلي، مرجع سابق، ص166.

على المال دون رضا صاحب الشأن، فإن الجريمة تعتبر سرقة ومثال ذلك قيام شخص بادعائه بأنه يعمل في مصلحة التلفونات ووصوله إلى أحد المنازل بهدف إصلاح الهاتف، ومن ثم قيامة بأخذ المال الذي وجده جوار سماعة الهاتف.

ويجب كذلك أن يكون التسليم مقصودا به نقل حيازة المال كاملة، أما الحيازة الناقصة فيعاقب عليها بعقوبة السرقة أو خيانة الأمانة.

ويجب أن يكون تسليم المال لاحقا على استعمال وسائل الاحتيال، وقد يتم التسليم من صاحب المال، كما يمكن أن يتم من الغير كوكيل، بناء على رغبة صاحب المال دون استلزام أن تكون إرادة الغير معيبة، طالما تم التسليم برضا صاحبه[1].

أخيراً يجب أن تقوم علاقة سببية بين الوسائل الاحتيالية التي استعملها الجاني، وتسليم المجني عليه للأشياء التي معه، بعبارة أخرى يجب أن يكون التسليم قد تم نتيجة لوسائل التدليس الجنائي التي لجأ إليها الجاني، والإيهام الذي ولده في نفس المجني عليه وترتب عليه تسليم المال [2].

ب- الركن المادي في جريمة النصب في مجال المعلوماتية

لإيضاح الركن المادي في جريمة النصب في مجال المعلوماتية لابد من مقارنتها بعناصر الركن المادي، وفقا للقواعد العامة التي سبق إيضاحها لمعرفة مدى تحققها لجريمة النصب في مجال المعلوماتية، وتلك العناصر تتمثل بالطرق الاحتيالية وسلب مال الغير ورابطة السببية.

والطرق الاحتيالية في مجال المعلوماتية تتمثل في الحالات التي يتوصل فيها شخص عن طريق التلاعب في منظومة المعالجة الإلكترونية للبيانات إلى الاستيلاء على مال الغير، كان يتلاعب في البيانات المدخلة، أو المخزنة داخل الحاسوب، أو في برامجه لاستخراج شيكات تدفع له، أو لتحويل كل أو بعض أرصدة الغير أو الفوائد المستحقة لهم إلى حسابه، أو التلاعب في الإشارات الإلكترونية المرتدة من الحاسوب المركزي إلى جهاز الصراف الآلي للنقود لاختلاس الأموال من أرصدة العملاء أو من رصيد جهاز الصراف نفسه، دون التأثير في بيانات الحاسوب المركزي، وفي حسابات

(1) حسني الجندي، مجدي محمد عقلان، مرجع سابق، ص295.
(2) حسن علي مجلي، مرجع سابق، ص159، وص314.

العملاء(1)، فهل بالإمكان الاحتيال على جهاز الحاسوب وإيقاعه في الغلط ؟ ومدى اعتبار التحويل الإلكتروني للأرصدة من حساب إلى آخر محققا النتيجة غير المشروعة المتمثلة بتسليم المال(2).

وحول مدى إمكانية وقوع فعل الاحتيال في مجال المعلوماتية، فإنه لا توجد مشكلة في وقوع جريمة النصب بطرق الاحتيال، إذا ما قام الجاني مستخدما تلك الطرق لإيهام المجني عليه بتسليمأي ٍ من المكونات المادية للحاسوب، أو الدعامة المادية المثبت عليها برنامج أو أكثر من برامج الحاسوب الآلي.

وإنما تثار المشكلة في حالة قيام الجاني باستخدام إحدى الطرق الفنية التي تستخدم في ارتكاب الجريمة في مجال المعالجة الآلية للمعطيات، وكذلك في حالة الاستخدام التعسفي لبطائق الائتمان الممغنطة، فهل بالإمكان الاحتيال على نظام الحاسوب الآلي وإيقاعه في الغلط باستخدام الطرق السالف ذكرها؟

وبهذا الخصوص لقد تبين لدى البعض أن فعل الاحتيال بطرقه المعروفة لا يقع على الحاسوب، لأن فعل الاحتيال لا يقع إلا على شخص طبيعي، ومرد ذلك أن قابلية نصوص النصب للتطبيق الذي يباشر على أنظمة الحاسوبات، يتوقف على شرط مفاده

(1) تتعدد الوسائل التي يتم بواسطتها عمليات الاحتيال الإلكتروني وأهمها :

- التلاعب في البيانات في مرحلتي الإدخال أو الإخراج، ويكون التلاعب في البيانات في مرحلة الإدخال قبل وأثناء إدخالها إلى نظام الحاسوب، حيث تتمثل عملية الإدخال (Input) في تغذية الحاسب الآلي ونظامه بالبيانات والمعلومات المراد معالجتها آليا، سواء تمثل ذلك في تغيير جزء أوكل البيانات والمعلومات المراد إدخالها إلى النظام أم حذف جزء من المعلومة أو عدة أجزاء أو المعلومة بكلها، أم اقتصر الأمر على إعاقة المعلومة كأن يتم إدخال المعلومة مع إخفائها، وبالتالي تنعدم الفائدة منها، أما التلاعب في البيانات في مرحلة الإخراج فتتم عن طريق التلاعب بالبيانات في مرحلة ما قبل الإخراج، بمعنى أن المعلومات قد تم إدخالها صحيحة وتم التلاعب بها قبل أن يتم إخراجها، سواء بطباعتها أو تخزينها بواسطة وسائط التخزين.
- التلاعب في البرامج: وهو ما يعد الاحتيال المعلوماتي بحق لتميزه بقدر كبير من التعقيد ولصعوبة اكتشافه، وتتم إما عن طريق تعديل في البرامج التطبيقية القائمة في المؤسسة بإدخال تعديلات غير مرخص بها على البرامج تساعد الجاني على إتمام جريمته، وقد يتم إجراء التعديلات عن طريق برامج الفيروسات، كما قد يتم التلاعب بالبرامج عن طريق تطبيق برامج إضافية يتم كتابتها عن طريق الجناة مسبقا، وقد تكون معدة مسبقا وتهدف إلى تعديل البيانات في الحواسيب الآلية، ومثال ذلك قيام مبرمج في إحدى البنوك في الولايات المتحدة الأمريكية بإدراج تعديلات على أحد البرامج بحيث يتم إضافة عشره سنتات إلى كل خدمة تقل قيمتها عن عشرة دولارات، ودولار إلى الخدمات التي تزيد قيمتها عن هذا المقدار، ثم تحويل تلك المبالغ تحت اسم وهمي، وقد تمكن من سحب العديد من المبالغ، ولم يتم اكتشاف أمره إلى عن طريق الصدفة حينما أراد البنك تكريم أول وآخر عميل له واكتشف أثناء ذلك أن العميل الأخير لا يوجد أصلا.
- التلاعب في البيانات التي يتم تحويلها عن بعد: وفي هذه الحالة يكفي أن يقوم الجاني بواسطة حاسوبه متصلا بوحدة التشغيل المركزية عن طريق شبكة الخطوط الهاتفية العادية أو غير ها من وسائل الاتصالات، حيث يتمكن الجاني من داخل منزله إتمام فعله مستخدما لوحدته الطرفية دون حاجة إلى الدخول إلى المؤسسة المجني عليها، سواء أكانت المؤسسة داخل الدولة أم خارجها بسبب الاتصالات الدولية التي أضحت تسهم في نشوء الجريمة المعلوماتية متعددة الحدود .لمزيد من التفصيل حول وسائل الاحتيال الالكتروني راجع: نائلة عادل محمد فريد فورة، مرجع سابق، ص435 وما بعدها.

(2) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مرجع سابق، ص370.

أن يكون الجاني قد خدع الشخص الذي يقوم بفحص ومراجعة البيانات[1]، فالوسائل الاحتيالية تفترض وجود الجاني والمجني عليه، وقيام الجاني باستخدام الطرق الاحتيالية، وفي مثل هذه الحالة فإن مالك النظام لا يكون موجودا وقت ارتكاب الجريمة، كما أن المجني عليه لم يكن موجودا ولم يتم التسليم بإرادته [2].

رأى آخر: بأنه يمكن وقوع فعل الاحتيال على أنظمة الحواسيب، حيث أن خداع أنظمة الحواسيب تتحقق بها الطرق الاحتيالية بمفهومها المستقر ككذب تدعمه أعمال مادية أو وقائع خارجية، فتتحقق الطرق باستخدام الجاني المستندات غير الصحيحة التي يخرجها الحاسوب، بناء على ما وقع في برامجه أو في البيانات المخزنة بداخلة من تلاعب، وأن النظام المعلوماتي ليس سوى وسيط للتحايل[3]، كما يمكن استخدام الأساليب الفنية في الاحتيال على النظام المعلوماتي في حالة استخدام النظام كأداة سلبية، ومثال ذلك قيام الجاني بالدخول على النظام باعتباره المستخدم الشرعي عن طريق الحصول على الرقم السري للمستخدم الشرعي، من أجل الاستيلاء على الأموال، وفي هذه الحالة تتحقق جريمة النصب باستخدام إحدى الطرق الاحتيالية وهي الاسم الكاذب الذي تم الدخول به إلى النظام من قبل الجاني الذي قام باستخدام الجهاز موهما الغير بأنه صاحب الاسم الحقيقي [4].

كذلك يمكن استخدام النظام المعلوماتي كاداه ايجابية عن طريق التدخل المباشر في المعطيات والكيان المنطقي، وذلك بإدخال معطيات وهمية أو تعديل البرامج أو خلق برامج صورية وهي جميعها طرق احتيالية، ومثال ذلك ما قامت به شركة تامين أمريكية من إعداد 64000 وثيقة تامين وهمية [5]، فلا يوجد شيء يمنع من وقوع الاحتيال على الكمبيوتر وبالتالي وقوع جريمة النصب بالاستيلاء على مال منقول مملوك للغير[6].

(1) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص272.
(2) أحمد خليفة الملط، مرجع سابق، ص402، وقد ورد هذا الرأي أيضا في مؤلف آمال قارة: الجريمة المعلوماتية، رسالة ماجستير قدمت إلى كلية الحقوق، بن عكنون، جامعة الجزائر، 2004، ص96.
(3) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 275.
(4) جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، بدون تاريخ طبعة، النهضة العربية للنشر، القاهرة، 2003، ص78.
(5)راجع: أحمد خليفة الملط ، مرجع سابق، ص404 .
(6) وتطبيقا لذلك فقد ذهب القضاء الكويتي في أحد أحكامه إلى وقوع جريمة النصب من المتهمة التي استولت على كرت السحب الآلي للمجني عليه بالإضافة إلى رقمه السري، وقامت بسحب مبلغ مالي من حساب صاحب الكرت، حيث اعتبرت محكمة التمييز الكويتية أن ما قامت به المتهمة من انتحال لصفة غير صحيحة تتمثل بأنها هي صاحبة الحساب أو وكيلة عنه، وقضت بوقوع جريمة نصب تامة في هذه الحالة، لمزيد من التفصيل=

وتتمثل النتيجة الإجرامية المبنية على فعل الاحتيال بالاستيلاء على مال المجني عليه، أي أن فعل الاحتيال الذي قام به الجاني باقترافه مستغلا طرق احتيالية من شأنها إيهام المجني عليه بصحة التصرف الذي يقدم عليه، بحيث يعتقد أن ذلك التصرف لا يشوبه أدني شك في سلامته، وبالتالي يقدم على تسليم المال للجاني عن طواعية واختيار، وتلك هي النتيجة الإجرامية لفعل الاحتيال.

وكما سبق التنويه إلى أنه يشترط في محل التسليم أن ينصب على مال مادي، وفقا للقواعد العامة لجريمة النصب، فهل تتوافر صفة المال المادي في النقود البنكية والكتابية بحيث يمكن تطبيق النصوص الجنائية لجريمة النصب عليها ؟ بمعنى آخر، هل ما يتحقق من استيلاء على النقود البنكية والكتابية عن طريق ما يعرف بالقيد الكتابي الناتج عن التلاعب في البرامج والبيانات والتي يتم من خلالها تحويل كل أو بعض أرصدة مالكيها أو فوائدها على حساب المتلاعب يعد بمثابة الاستيلاء على الأموال في جريمة النصب ؟ وهل يتحقق التسليم في حالة إساءة استخدام بطاقات الائتمان من قبل حاملها أو من قبل الغير كما هو في جريمة النصب ؟

1) الاستيلاء على النقود الكتابية والبنكية

برز الخلاف بين الفقهاء بشأن الاستيلاء على النقود الكتابية والبنكية التي يتم الاستيلاء عليها عن طريق القيد الكتابي، وذلك في حالة قيام الجاني بالتلاعب في البيانات المخزنة في النظام المعلوماتي أو في برامجه لتحويل الأموال إلى حساب الجاني:

- أن جريمة النصب تقوم بموجب الاستيلاء على النقود البنكية والكتابية عن طريق القيد الكتابي، وقد أرست هذا النهج محكمة النقض الفرنسية عندما ابتكرت نظرية التسليم المعادل وذلك على إثر قضاها في مواجهة حالات نصب تتمثل في إيهام عداد موقف انتظار السيارات والتلفونات بصحة القطع المعدنية، وقد لاقت هذه النظرية ترحيبا واسعا لدى أغلب الفقه الفرنسي لمواجهة حالات الاحتيال على نظام الحاسوب[1].

=راجع: حكم محكمة التمييز الكويتية، 28/5/ 1990، ص204/ 89 جزائي، مجموعة القواعد التي أوردتها محكمة التمييز ،1/1/1996، ص32، مشار إليه لدى شيماء عبد الغني محمد عطا الله : الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، 2005 ، ص79.

(1) محمد سامي الشواء، ثورة المعلومات وانعكاساتها على قانون العقوبات،مرجع سابق، ص131، وص132.

فالتسليم وفقا لأصحاب هذا الرأي ومن يؤيده[1]، لا يثير مشكلة باعتباره عملا قانونيا عنصره الجوهري إرادة المجني عليه المعيبة بالخداع، والمناولة ليست سوى مظهر مادي لهذا العمل، وتسليم المال في جريمة الاحتيال المعلوماتي تتوافق مع ذلك، حيث تتم بكل عمليات حسابية يقوم بها الحاسوب الآلي بحيث لا يصل المال إلى يد الجاني بصورة مباشرة، فالعبرة بقيام الحاسوب الآلي بوضع المال محل النشاط الإجرامي تحت تصرف الجاني بسبب الأساليب الاحتيالية التي مارسها.

- يمكن وقوع جريمة النصب بالاستيلاء على النقود الكتابية أو البنكية بمجرد القيام بالقيد الكتابي الناتج عن التلاعب بالبرامج والبيانات، إلا أن أصحاب هذا الاتجاه يبررون ذلك بأن تلك النقود الكتابية تعد أموال مادية مثلها مثل الأموال النقدية وبالتالي تسري عليها عقوبة جريمة النصب وفقا للقواعد العامة في القانون الجنائي[2].

- **أن** عدم وقوع جريمة النصب على النقود البنكية أو الكتابية إذا تم الاستيلاء عليها عن طريق القيد الكتابي، لكون تلك النقود لا تعد من قبيل الأموال المادية، وتعد من قبل الديون والاستيلاء لا يتحقق إلا على مال [3].

2) الاستعمال غير المشروع لبطاقة الائتمان

قد يقع استخدام البطاقة الائتمانية بطريق الغش من المالك الشرعي لتلك البطاقة، وقد يقع ذلك من قبل الغير، فهل يعد الاستخدام الغير شرعي لبطائق الائتمان داخلا في جريمة النصب؟

أ) استعمال البطاقة من مالكها الشرعي

لمعرفة حكم الاستخدام غير الشرعي لبطاقة الائتمان لابد من التفرقة بين ثلاث حالات:

---

(2) نائلة عادل محمد فريد قورة، مرجع سابق، ص465.

(2) هذا الرأي يجد له مسوغا في عدد من التشريعات ومنها تشريعات، كندا وفقا للمادة (2/282 ق.ع) ، والمواد(312،311،310،من ق.ع الهولندي)، والمواد(137، 140 ، 141 ،من ق.ع السويسري) وكذلك في تشريعات الولايات المتحدة الأمريكية، و إنجلترا، وبهذا الخصوص فقد قضت المحكمة العليا بالنمسا مؤخرا بأن تعبير المال الوارد بالمادة (133) من ق.ع الخاصة بجريمة خيانة الأمانة، والمادة (134) ألخاصة بالاحتيال يشمل النقود الكتابية، ويؤيد هذا الرأي من الفقه العربي الدكتور أحمد خليفة الملط ، مرجع سابق، ص416.

(3) ومن التشريعات التي انتهجت في قوانينها العقابية هذا الاتجاه القانون آلياباني والقانون الألماني وقانون دولة لوكسمبورج حيث نصت على اعتبار النقود الكتابية بمثابة ديون لا تخضع لعقوبة جريمة النصب، ومن أنصار هذا الرأي في الفقه العربي، عفيفي كامل عفيفي، مرجع سابق، ص156.

(1) السحب بواسطة البطاقة بما يتجاوز الرصيد

اعتبر البعض بأن السحب بواسطة البطاقة بما يتجاوز الرصيد يشكل جريمة سرقة بينما اعتبره آخرون يشكل جريمة نصب، إلا أن محكمة النقض الفرنسية اعتبرته إخلالا بالتزام تعاقدي [1].

(2) استعمال البطاقة في السحب بالرغم من إلغائها

يشكل هذا السلوك لدى البعض جريمة النصب في حالة استخدام البطاقة الملغاة في الوفاء للتجار، باعتبار أن تقديم البطاقة يهدف إلى الاقتناع بوجود ائتمان وهمي لا وجود له في الواقع، إذ أن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان[2].

أما في حالة استخدام البطاقة الملغاة في سحب النقود فيرى البعض[3] بأن ذلك لا يشكل جريمة لأن البرنامج المطبق على أجهزة السحب الآلي للنقود يقوم بسحب البطاقة أو رفضها، إذ أصبح سحب النقود بموجب البطاقة الملغاة أمراً غير متصور، حيث ترتبط الموزعات بحسابات العملاء، وبالتالي فإنها سترفض تسليم أوراق البنكنوت التي يطلبها الحامل إذا كانت تزيد عن رصيده الجاهز في البنك.

بينما يرى البعض الآخر أن استعمال مالك البطاقة الملغاة لتلك البطاقة في سحب النقود من أجهزة السحب الآلي تقوم به جريمة نصب باستخدام صفة غير صحيحة، حيث يؤدي إلغاء البطاقة إلى تجريد الحامل من صفته كحامل شرعي لها[4]. كما أن هذا السلوك في نظر البعض يهدف إلى الإقناع بوجود أيتمان وهمي لا وجود له في الواقع[5].

---

(1) راجع: آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص51. وراجع أيضا هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص110، والمؤلفة- الأخيرة- تخالف رأى محكمة النقض الفرنسية باعتبار أن الفعل يكمن في مجرد إخلال بالتزام تعاقدي فحسب، حيث ترى بأن الواقعة تكيف على أنها سرقة وليست نصب أو خيانة أمانة، لانعدام الطرق الاحتيالية، وانعدام الصفة غير الحقيقة، وغياب أي عقد من عقود الأمانة، فصاحب الكرت هو المالك الشرعي له، وهي تشبه حالة المدين الذي يعطي الدائن حافظة نقوده ليأخذ منها دينه فيستقطع أكثر من المبلغ الذي يستحقه.

(2) جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطائق الائتمان الممغنطة، مرجع سابق، ص80.ومن القضايا التي وردت في نفس المؤلف قيام أحد المتعاملين في فرنسا في التعسف في استخدام بطاقته الائتمانية مما جعل البنك مصدر البطاقة يلغيها ويطلب من العميل ردها، ونظرا لكون العميل لم يقم بردها، واستمر في استعمالها في الوفاء فقد رفع البنك دعوى أمام محكمة جنح باريس، حيث قضت بإدانة العامل بتهمة النصب على أساس تقديمه بطاقة مجردة من أي قيمة، لأنها ملغاة بواسطة البنك المصدر لها، وأن ذلك يهدف إلى الإقناع بوجود ائتمان وهمي، والحصول من البنك على الوفاء للتجار الذين قدموا سلعا لحامل البطاقة مما يشكل استيلاء على بعض ثروة الغير.

(3) مشار إلي هذا الرأي في مؤلف جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، مرجع سابق، ص82.

(4) راجع: جميل عبد الباقي الصغير، مرجع سابق، ص83.

(5) وقد ورد هذا الرأي في مؤلف عفيفي كامل عفيفي، مرجع سابق، ص83.

(3) استعمال البطاقة للسحب بالرغم من انتهاء صلاحيتها

اعتبر البعض هذا السلوك يكون جريمة خيانة أمانة، على أساس أن البطاقة بمثابة محرر يتم تسليمها للعميل على سبيل عارية الاستعمال[1]، فلا يعد هذا السلوك مكونا لجريمة نصب، فبالإضافة إلى سذاجة الأسلوب في كون التاجر ملزما بقراءة البطاقة منتهية الصلاحية، وبالتالي رفضها، بحيث لا يمكن تحقق جريمة النصب إلا في حالة تواطؤ التاجر مع حامل البطاقة بعمل فواتير غير سليمة، يتم من خلالها الإيهام بعدم انتهاء صلاحية البطاقة، فحامل البطاقة وإن انطوى سلوكه على كذب فيما يتعلق بمدة صلاحية البطاقة فإظهار البطاقة ليس كافيا لتحقق الطرق الاحتيالية، حيث إن هذا المظهر الخارجي المتمثل بتقديم أو إظهار البطاقة هو الذي أنتج الكذب المتعلق بمدة صلاحيتها[2].

بينما اعتبرها البعض الآخر تشكل جريمة نصب في حالة ما إذا نجح حامل البطاقة منتهية الصلاحية في إدخالها جهاز الصراف الآلي، وبدلا من أن يبتلعها أو يرفضها تم التحايل عليه باستخدام رقم سري خاص ببطاقة أخرى، وتوصل بذلك إلى سحب النقود، بينما لا تعد جريمة نصب فيما عدا ذلك[3].

ب) الاستعمال غير المشروع لبطاقة الائتمان من قبل الغير

الاستعمال غير المشروع لبطاقة الائتمان من قبل الغير قد يتم من خلال استعمال بطاقة الغير المسروقة أو المفقودة.

فاستعمال البطاقة المفقودة أو المسروقة بواسطة الغير في الوفاء لإتمام المعاملات التجارية تتوافر به الطرق الاحتيالية لجريمة النصب، والتي تهدف إلى إقناع التاجر، أو إيهامه بوجود ائتمان وهمي من أجل الاستيلاء على أموال الغير، وتكتمل الجريمة بحدوث عملية التسليم بواسطة التاجر.

كما أن استعمال الغير للبطاقة المفقودة أو المسروقة لسحب النقود، تتحقق به جريمة النصب ويكتمل النشاط بالحصول على النقود، أما إذا أقتصر الفعل على المحاولة دون

---

(1) محمد سامي الشواء، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص115، مشار إليه لدى آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص51.
(2) نائلة عادل محمد فريد قورة، مرجع سابق، ص52.
(3)جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطائق الائتمان، مرجع سابق، ص88.

تحقق النتيجة المتمثلة بتسليم البضاعة أو سحب النقود فإن الأمر يقتصر على جريمة الشروع في النصب[1].

كما أن استعمال بطاقات الائتمان المزورة، يعد من قبيل الطرق الاحتيالية التي تقوم عليها جريمة النصب [2]. ويعتبرها البعض جريمة سرقة باستخدام مفتاح مصطنع يقوم بدور بفتح الآلة، كما يعتبر هذا الرأي أن استخدام البطاقة المفقودة أو المسروقة من قبل الغير جريمة سرقة وليست نصبا، لقيام المستخدم باختلاس مال الغير، وأن الاستيلاء على الأشياء المفقودة بنية التملك يعتبر سرقة[3].

وإزاء الخلاف القائم حول تكييف، استخدام البطاقة من قبل صاحبها لسحب أكثر من الرصيد، أو السحب مع أنها قد أصبحت ملغاة، أو انتهت مدة صلاحيتها، أو استخدام البطاقة المفقودة أو المسروقة من قبل الغير، بجريمة نصب أو خيانة أمانة أو سرقة، أو إخلال بالتزام تعاقدي، ونظرا لكون الجرائم قد ارتبطت بظهور هذا النوع من البطائق، فنرى اعتبارها من الجرائم المستحدثة التي ظهرت وتطورت بظهور التكنولوجيا الرقمية وعلم الاتصالات، ولابد من نصوص قانونية تتضمن الحماية الجنائية لإساءة استخدام تلك البطائق بما يخالف الهدف من إصدارها.

3- الركن المعنوي لجريمة النصب

النصب جريمة عمدية لا تقوم إلا بتوافر القصد الجنائي العام، أي انصراف إرادة الجاني إلى تحقيق وقائع الجريمة مع العلم بأركانها[4]

فمن ناحية أولى يجب أن يكون الجاني عالماً بكل العناصر المكونة للاحتيال، وأن يدرك أن من شأن تلك الوسائل التأثير على المجني عليه وحمله على تسليم أمواله[5].

ومن ناحية أخرى يجب أن تتجه إرادة الجاني إلى استعمال إحدى أساليب الاحتيال المنصوص عليها في القانون، وأن تنصرف إرادة الجاني إلى تحقيق النتيجة غير المشروعة والمتمثلة بالاستيلاء على مال الغير.

---

(1) راجع: سامح محمد عبد الحكم، الحماية الجنائية لبطاقات الائتمان، دار النهضة العربية، القاهرة، 2003، ص84، وص85.
(2) سامح محمد عبد الحكم، نفس المرجع، ص84.
(3) هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقار، مرجع سابق، ص114.
(4) نزية نعيم شلال، دعاوي الاحتيال وما جرى مجراه، المؤسسة الحديثة للكتاب، طرابلس- لبنان، 2001، ص8.
(5) علي حسن مجلي، مرجع سابق، ص173.

وجريمة النصب في مجال المعلوماتية شأنها شأن جريمة النصب التقليدية، جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي، فيجب أن يتوافر القصد الجنائي العام المتمثل بالعلم والإرادة إلى جانب القصد الجنائي الخاص.

فيجب أولا: أن يعلم المتهم أن المعلومات - سواء أكانت في مرحلة الإدخال أم الإخراج - أو البرامج التي يقوم بالتلاعب فيها يكون من شأنها أن تجعل نظام الحاسوب يستجيب لها، فيقوم بتنفيذ ما يعهد إليه من تعليمات تهدف إلى تحقيق الاحتيال المعلوماتي لتحقيق الربح غير المشروع.

كما يجب أن يعلم أن المال الذي يستولي عليه بواسطة الاحتيال المعلوماتي مملوك للمجني عليه أو لشخص آخر غيره.

ويجب ثانيا: أن تتجه إرادة الجاني الحرة والمدركة إلى القيام بتلك الأفعال الاحتيالية.

كما يجب إضافة إلى ذلك تحقق القصد الجنائي الخاص حسب رأي جانب من الفقه، ويأخذ به البعض، حيث يشترط أن تتجه إرادة المتهم إلى تحقيق ربح غير مشروع له أو لغيره[1]. وفقا لما سارت عليه عدد من القوانين الحديثة[2].

بخلاف آخرين حيث لا يشترط في نظرهم تحقق القصد الجنائي الخاص في جريمة الاحتيال المعلوماتي، لأن إرادة التملك للمال ما هو إلا نتيجة للاحتيال، ونية التملك لا تمثل غاية خاصة تخرج عن نطاق العناصر التكوينية للجريمة [3].

ويستنتج مما سبق بأن القانون اليمني لم يتضمن نصوصا قانونية تنظم تجريم وعقاب جرائم الإعلام الآلي ومنها جريمة النصب في مجال المعلوماتية، لذلك فقد يتم تكييف قضية نصب في مجال المعلوماتية على أنها سرقة[4]، وكذلك القانون الجزائري،

---

(1) نائلة عادل محمد فريد قورة ، مرجع سابق، ص488.
(2) ومن تلك القوانين التي تطلبت في جريمة الاحتيال المعلوماتي القصد الجنائي الخاص المتمثل في تحقيق الربح غير المشروع، القانون الفدرالي الأمريكي لجرائم الحاسبات الآلية وفقا للمادة(1030) فقرة(أ) بند(4) ،وقانون العقوبات الألماني المادة (263 –أ) والتي تضمنت شرط أن يكون الفعل بنية تحقيق ربح غير مشروع للجاني أو لغيره، وكذلك قانون العقوبات اليوناني حيث تطلب في أن تتم أفعال الاحتيال بنية تحقيق إثراء للفاعل أو لغيره بربح غير مشروع وفقا لنص المادة(263 فقره أ).راجع نائلة عادل محمد فريد قورة، مرجع سابق، ص490.
(3) آمال عبد الرحيم عثمان، شرح قانون العقوبات المصري، القسم الخاص، ص540. مشار اليه في مؤلف نائلة عادل محمد فريد قورة،المرجع السابق،ص488.
([4]) في حكمين قضائيين يمنيين تم تكييف قضية التلاعب بمعطيات الحاسوب وتحويل أموال، بجريمة سرقة بتبرير أنه تم اخذ المال خفيه ومن حرز مثله وهي كلمة المرور، مع أن التكيف الأنسب لها جريمة نصب، باعتبار أن تحويل الأموال كان نتيجة للتحايل على نظام الحاسوب، وأن الحرز المعتبر في جريمة السرقة هو حرز مادي لا =

حيث لم يتضمن تجريم الاعتداء على أنظمة الإعلام الآلي، أو المعطيات المعالجة آليا بنصوص صريحة حتى نوفمبر 2004 بالرغم من وجودها من الناحية العملية، و كان القضاء يلجأ إلى تكييفها طبقا للجرائم والجنح التقليدية، كالنصب والسرقة وخيانة الأمانة ماعدا سرقة المعلومات التي كيفها على أساس الاعتداء على حقوق المؤلف [1].

كما أن القانون الجزائري في تعديله الأخير الذي من خلاله تم إضافة قسم سابع يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات لم يتضمن نصوصا قانونية تتعلق بجريمة الاحتيال المعلوماتي [2]، وكذلك القانون رقم (09-04) بخصوص الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما لعام 2009، حيث اقتصر على نص عام يدخل الجرائم التقليدية المرتكبة بواسطة المعلوماتية في إطار التجريم، وبالتالي كان لابد من الرجوع للنص القانوني المتعلق بجريمة الاحتيال في قانون العقوبات[3] لبيان مدى إمكانية تطبيقه على الاحتيال في مجال المعلوماتية؟

فبالإضافة إلى رأي بعض الفقهاء في الجزائر المؤيد لموقف القضاء الجزائري من تطبيق نصوص جريمة النصب على النصب في مجال المعلوماتية وذلك قبل تضمين القانون الجزائري جرائم الإعلام الآلي ضمن نصوصه، حيث كانت تكييف طبقا للجرائم والجنح التقليدية، وبالتالي فلا يوجد ما يمنع من بقاء ذلك التكييف بالنسبة لجريمة النصب وخيانة الأمانة، طالما قد خلت النصوص الجديدة في القانون من تضمينها .

=كيانات منطقية. وتتمثل القضية في قيام أحد الموظفين في شركة كنديان نكسن بتروليم يمن بالدخول والتلاعب بالمعطيات المخزنة في نظام المعالجة الآلية للمعطيات الخاص بالشركة، مستغلا اسم وجهاز وكلمة المرور الخاصة بأحد زملائه أثناء فترة أجازته، والذي يقتصر عمله على إدخال البيانات الخاصة بالتحويلات الإلكترونية، وكذلك أسم وكلمة المرور الخاصة بأحد الأشخاص الذين يقومون بالمصادقة على التحويلات، بحيث أن عمل الثاني مكمل للأول فبينما يقوم الأول بإدخال البيات، فإن عملية التحويل لا تتم إلا بالمصادقة عليها من الأخر، وقد قام الجاني بعمل الشخصين حيث أدخل بيانات تتعلق بتحويل مبلغ ثلاثة مليون وأربعون ألف وستمائة وسبعة وعشرون دولار أمريكي، والمصادقة على عملية التحويل وذلك من بنك أوف أمريكا في الولايات المتحدة الأمريكية إلى بنوك في ماليزيا بأسماء أشخاص تم الترتيب معهم بالسفر وتحويل جزء من تلك المبالغ إلى بنوك في اليمن بأسماء آخرين، وقد تم أدانتهم بجريمة سرقة مال منقول مملوك للمجني عليها شركة كنديان نكسن بتروليم يمن، وإن لم تحكم محكمة أول درجة وكذلك محكمة الاستئناف بعقوبة جريمة السرقة بسبب صدورعفو رئاسي بشرط إعادة المبالغ التي تم تحويلها وقبول الشركة بذلك. لتفاصيل أكثر حول وقائع القضية راجع: حكم المحكمة الجزائية المتخصصة الابتدائية رقم (7) في القضية الجزائية رقم (29) بتاريخ 2005/5/14، وحكم المحكمة الجزائية الأستنافية المتخصصة رقم (27) في القضية الجزائية رقم (13) بتاريخ 2005/9/20، وقد حصل الباحث على نسخة من الحكمين من المحكمة لكونهما غير منشورين.

(1) نصرون وردية، مرجع سابق، ص9.

(2) القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004.

(3) راجع: المادة (372) من قانون العقوبات الجزائري.

فلا يوجد ما يحول دون دخول البرامج والبيانات تحت طائلة النصوص التقليدية، سواء باعتبارها أموالا أم منقولات، ولذلك فلقد أصبح من المتصور أن يقوم أحد الأشخاص بالتلاعب بها، وتحويل النقود الالكترونية لصالحة بطرق احتيالية أو باتخاذ اسم أو صفة غير صحيحة[1]، وذلك ما دفع العديد من الدول إلى النص صراحة على صلاحية النقود الإلكترونية لان تكون محلا لجرائم الأموال، بالرغم من طبيعتها غير المادية وحبذا لو اعتمد المشرع الجزائري ذلك الحل[2]

أخيرا وإزالة للالتباس والاختلافات الفقهية بصدد التكييف القانوني لجريمة النصب في مجال المعلوماتية فإن على المشرع اليمني والمشرع الجزائري تضمين جريمة النصب في مجال المعلوماتية في قانون العقوبات، من خلال نصوص خاصة يتم إلحاقها بالنسبة للقانون الجزائري بالقسم السابع من ق.ع الخاص بالمساس بأنظمة المعالجة الآلية للبيانات، ويتم تضمينها في القانون اليمني في قسم خاص بالجريمة المعلوماتية كما فعلت عدد من التشريعات الحديثة[3]. ومن القوانين العربية التي نصت على جريمة الاحتيال المعلوماتي نظام مكافحة الجرائم المعلوماتية السعودي[4].

([1]) ومع ذلك فقد تم تكييف قضية التلاعب بمعطيات الحاسوب وتحويل أموال، بجريمة سرقة بتبرير أنه تم اخذ المال خفيه ومن حرز مثله وهي كلمة المرور، مع أن التكيف الأنسب لها جريمة نصب، باعتبار أن تحويل الأموال كان نتيجة للتحايل على نظام الحاسوب، وأن الحرز المعتبر في جريمة السرقة هو حرز مادي لا كيانات منطقية. لتفاصيل أكثر راجع: حكم المحكمة الجزائية المتخصصة الابتدائية رقم (7) في القضية الجزائية رقم (29) بتاريخ 2005/5/14، وحكم المحكمة الجزائية الأستئنافية المتخصصة رقم (27) في القضية الجزائية رقم (13) بتاريخ 2005/9/20

(2) آمل قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص31.

(3) ومن تلك القوانين، القانون الفدرالي الأمريكي لجرائم الحاسبات الآلية، وقانون العقوبات الألماني، وكذلك قانون العقوبات اليوناني .راجع نائلة عادل محمد فريد قورة، مرجع سابق، ص490.

(4) نصت المادة(4) من نظام مكافحة الجرائم المعلوماتية السعودي على جريمة النصب المعلوماتي بقولها(يعاقب بالسجن مدة لاتزيد عن ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية

- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صيحة.
- الوصول ـ دون مسوغ نظام صحيح ـ إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

الفصل الثاني

الجرائم المعلوماتية المستحدثة

new Information Crimes

نتج عن انتشار المعلومات (Information) وتدفقها غير المحدود، واتساع النظام المعلوماتي وتدخله في مجالات الحياة المختلفة، أن تطور أسلوب ارتكاب الجرائم المعلوماتية (Information crimes) ضد الأموال، والأشخاص، والنظم بحد ذاتها، وظهرت جرائم معلوماتية مستحدثة نتيجةً للتطور التقني لم يتناولها القانون الجنائي التقليدي، مما أجمع معه مشرعوا القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام الحاسب الآلي وشبكة الإنترنت، ودفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة، وما أثارته من مشكلات قانونية حول تطبيق القانون الجنائي، وقد انعكس ذلك على تشريعات بعض الدول، حيث دفع بعضها إلى إيجاد قوانين مستقلة، ودفع البعض الآخر إلى إضافة نصوص قانونية إلى قوانينها - سواء في شقها الموضوعي أم الإجرائي - لمواجهة تلك الجرائم، تناولت تجريم ذلك النوع المستحدث من الإجرام، وبينت القواعد الإجرائية المتبعة لكشف تلك الجرائم ومعاقبة مرتكبيها، وبالرجوع إلى قوانين الدول العربية يلاحظ بأن معظم قوانينها لا تتضمن نصوصاً قانونية مستحدثة لمواجهة الإجرام المعلوماتي، باستثناء الجزائر وقطر وسلطنة عمان، ودولة الإمارات العربية المتحدة، والمملكة العربية السعودية، حيث سارت الأولى والثانية والثالثة على نهج الدول التي أضافت نصوصاً تجريمية إلى قوانين العقوبات لمواجهة تلك الجرائم، بينما سارت الرابعة والخامسة على نهج الدول التي وضعت قانونا خاصا لمواجهة تلك الجرائم المعلوماتية، وأياً ما كان الأمر سواء مواجهة تلك الجرائم عن طريق تعديل التشريعات القائمة، أم عن طريق تشريعات مستقلة، فإن النتيجة في النهاية واحدة، وهي عدم ترك تلك الجرائم بلا عقوبات.

ولكون الدراسة تتعلق بالقانونين اليمني والجزائري، ونظراً لعدم وجود قانون خاص بالجرائم المعلوماتية (Information crimes)، أو نصوص خاصة يتضمنها قانون العقوبات اليمني تنظم كيفية مواجهة هذا النوع الجديد من الإجرام، مع أن هذه

الجرائم قد بدأت بالظهور في المجتمع اليمني(1)، فلا يكون أمامنا إلا أن نتناول أركان تلك الجرائم على ضوء النصوص القانونية في قانون العقوبات الجزائري ، حيث تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي بهدف حماية المجتمع الجزائري من هذه الظاهرة الخطيرة (2)، وعمل على استحداث نصوص قانونية تضمنها التعديل الأخير لقانون العقوبات(3) ، وسيتم الاستعانة بالقانون الفرنسي كلما أمكن ذلك لكون نصوص القانون الجزائري مستسقاة من القانون الفرنسي(4). كما سيتم إيضاح بعض الجرائم التي نص عليها القانون الفرنسي وأهملها الجزائري. وستقتصر الدراسة على أهم

---

(1) تم رصد ثلاث قضايا في الجمهورية اليمنية، منها جرائم معلوماتية وأخرى ارتكبت بواسطة المعلوماتية تتمثل **الأولى :** بقيام موظف في شركة كنديان نكسن بتر ليوم البترولية بالدخول إلى نظام معلوماتي غير مسموح بالدخول إليه من قبل ذلك الموظف، ومن ثم تحويل مبلغ 3,00,040,727 $ (ثلاثة مليون وأربعين ألف وستمائة وسبعة وعشرين دولاراً أمريكي من حساب الشركة في بنك أوف أمريكا إلى حساب تم فتحه بأسماء أشخاص آخرين في عدة بنوك في ماليزيا ومن ثم تحويلها إلى ثلاثة بنوك يمنية بأسماء آخرين، وتم استلام جزء من المبلغ وضبط الجناة .

وتتمثل الثانية : في جريمة قتل، تم التخطيط لها واستدراج الضحية عن طريق الإنترنت، تتمثل في قيام المتهم بالدخول في شبكة الإنترنت باسم فتاة والتعرف على شخص من محافظة أخرى غير محافظة المتهم ومن ثم قيامه بطلب شراء السيارة التابعة للمجني عليه، وعند وصول المجني عليه إلى الفتاة التي كانت تراسله عبر الانترنت تم استدراجه إلى المنزل، وكان الجاني يلبس لبس فتاة، وقام بإعطائه مشروباً كان قد دس السم فيه، ومن ثم القيام بقتله وكان الهدف أخذ السيارة، والثالثة قيام مجموعه من أصحاب محلات السيد يهات والأشرطة بترويج أفلام مخلة بالحياء ومنافية للآداب ألعامة، حيث تم ضبطهم بتاريخ 3/29 2007، وإغلاق عدد خمسه محلات ومصادرة الأشرطة التي تم ضبطها وسحب رخص مزاولة المهنة منها.

راجع في القضية الأولى : صحيفة 26 سبتمبر، العدد 1103، وصحيفة الجمهورية، ع14565، الاثنين 04 ديسمبر(كانون الأول) 2006 على الرابطين:

http://www.26sep.net/newsweekarticle.php?lng=arabic&sid=7394

http://www.algomhoriah.net/newsweekarticle.php?sid=31021&page=1

وفي الثانية : موقع المجلس اليمني وموقع منتديات صوت القران، ت.د 27-12-2006، 08:39 AM على الرابط:

http://www.al-yemen.org/vb/archive/index.php/t-166743.html

http://quran.maktoob.com/vb/quran9112

وفي الثالثة موقع صحيفة يمن نيوز، والبيانات الآن غير متاحة بسبب اختراق موقع الصحيفة وتدمير الأرشيف الخاص بها حيث كانت متاحة على الرابط

http://www.yemen-press.com/news572.html

(2) انتشرت الجرائم المعلوماتية في المجتمع الجزائري بشكل ملفت للنظر، إذ تقدر الإحصائيات المرصودة لتلك الجرائم، والتي منها الاعتداءات على النظم المعلوماتية مابين 200 إلى 250 اعتداء يوميا . آمل قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص100.

(3) جرم المشرع الجزائري المساس بأنظمة المعالجة الآلية للمعطيات في القسم السابع مكرر من القانون رقم (04 - 15) المؤرخ في 10 نوفمبر 2004 المُعدل والمُتمم للأمر رقم (66 - 156) المؤرخ في 8 / يونيو 1966 المتضمن قانون العقوبات.

(4) تعاقبت القوانين الفرنسية الخاصة بالمعلوماتية ومواجهة الجرائم الناتجة عنها، فقد أصدرت فرنسا في 6 / 1 / 1978 قانوناً يسمى بالمعلوماتية والحقوق الشخصية، وعقب ذلك صدر مرسوم في 23 / 12 / 1981 لتحديد بعض المخالفات المرتبطة بجرائم المعلومات، ثم أصدرت في عام 1988 قانوناً لحماية نظم المعالجة الآلية للمعطيات والمعلومات من المادة 462 إلى المادة 462 فقرة / 4، ثم صدر تعديل جديد للقانون في 1 / 3 / 1994، وبعد عشر سنوات من هذا التعديل تم تعديل قانون العقوبات الفرنسي عام 2004، وقد أضاف القانون لفرنسي بموجب هذا التعديل الأخير جريمة أخرى هي جريمة التعامل بوسائل يمكن أن ترتكب بها جريمة من الجرائم المعلوماتية المنصوص عليها في القانون ذاته، وقد نصت على هذه الجريمة المادة 323-3-1 ، راجع محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة ماجستير، دار الجامعة الجديدة، الإسكندرية، 2007، ص99.

تلك الجرائم وقد يأتي الحديث عن بقية الجرائم المعلوماتية أو ما ظهر منها في دراسات قادمة، لكون إيضاح كل الجرائم يحتاج أكثر من رسالة، بل إن بعضها قد تحتاج إلى دراسة لوحدها كالجرائم المرتبطة ببطائق الائتمان، أو التزوير المعلوماتي.

وقبل أن نتناول أحكام كل جريمة على حدة سوف نتناول في المبحث الأول الأحكام المشتركة لتلك الجرائم مجتمعة ، مع بيان أوجه القصور إن وجدت، فنصوص القانون في مجال المعلوماتية لابد أن تكون واضحة، كونه جديداً ومتميزاً في مصطلحاته[1].

وسيتم بيان موقف قانون العقوبات اليمني رقم 12لعام 1994م من تلك الجرائم، لإيضاح مدى إمكانية انطباق نصوصه على تلك الجرائم المهمة والخطيرة على الأمن القومي للدولة، وحياة وتعاملات المجتمع بشكل عام، أم أن الأمر يحتاج إلى إعادة النظر وإدراج نصوص قانونية في قانون العقوبات تعاقب على اقتراف تلك الجرائم.

([1]) هدى حامد قشقوش، جرائم الحاسب الالكتروني بالتشريع المقارن، دار النهضة العربية ، القاهرة ،1992،ص9.

المبحث الأول

الأحكام المشتركة للجرائم المعلوماتية

نظرا لخطورة الجرائم المعلوماتية والآثار الناجمة عنها، على مستوى الفرد والمجتمع والدولة، بل والمجتمع الدولي باعتبارها من الجرائم التي لا تعترف بالحدود الجغرافية، ويمكن ارتكابها في أكثر من دولة في آن واحد، فقد سعت التشريعات الحديثة كلا على حدة في وضع أحكام مشتركة تحول دون ارتكابها، وذلك بتجريم المراحل السابقة عليها كالشروع والاتفاق الجنائي.

كما شددت من عقوبات بعض الجرائم، منها الجرائم التي تمس الأمن الوطني للدولة، وضاعفت من عقوبات الجرائم عندما يتم ارتكابها من قبل الشخص المعنوي.

فالجرائم المعلوماتية تشترك بعدد من الأحكام، بعضها يتعلق بالجريمة والبعض الآخر يتعلق بالعقوبة.

أما الأحكام المشتركة التي تتعلق بالجريمة فتتمثل في تجريم الاتفاق الجنائي بغرض الإعداد لجريمة من الجرائم المنصوص عليها في القانون، وكذا تجريم الشروع في ارتكاب إحدى جرائم المعلوماتية.

فالاتفاق الجنائي والشروع في اقترف الجرائم من الأمور التي تشترك في أحكامها الجرائم المعلوماتية المستحدثة المنصوص عليها في قانون العقوبات الجزائري.

وبالنسبة للأحكام المشتركة المتعلقة بالعقوبة فقد ضاعف المشرع الجزائري من عقوبة الجرائم المعلوماتية في حالة أن تكون الجرائم المعلوماتية المرتكبة ضد المؤسسات والهيئات العامة، كما ضاعف عقوبة الغرامة إلى خمسة أضعاف في حالة ارتكاب جريمة من جرائم المعلوماتية من قبل الشخص المعنوي .

كما تشترك الجرائم المعلوماتية كذلك في أحكام العقوبات التكميلية، وسيتم تناول تلك الأحكام تباعا.

المطلب الأول
الاتفاق الجنائي في جرائم المعلوماتية

تضمن قانون العقوبات الجزائري في نصوصه المتعلقة بتجريم المساس بأنظمة المعالجة الآلية للمعطيات النص على جريمة الاتفاق الجنائي في مجال المعلوماتية[1]، وعدم الاكتفاء بالنصوص المتعلقة بجمعية الأشرار[2].

بخلاف ق.ج.ع.ي، حيث لم يتضمن نصوصاً تجرم الاتفاق الجنائي في الجرائم المعلوماتية، كما أنه لم ينص على جريمة الاتفاق في نصوصه التقليدية باستثناء الجرائم الماسة بالأمن القومي للدولة وذلك بموجب نص المادة (129) حيث نصت على أن:(من حرض أو اشترك في اتفاق جنائي لارتكاب إحدى الجرائم المنصوص عليها في هذا الفصل أو شرع في ارتكاب أي منها يعاقب بذات العقوبة المقررة لها، ولو لم يترتب على فعله اثر)[3]، وقد سبق إيضاح تلك الجرائم ضمن الجرائم الماسة بالأمن القومي للدولة أثناء تناول الجرائم التقليدية المرتكبة بواسطة نظم المعلوماتية.

وقد يعذر المشرع اليمني في عدم وضعه نصوصاً قانونية مستحدثة لمواجهة جريمتي الاتفاق في مجال المعلوماتية، كونه لم يقم باستحداث أو وضع نصوص قانونية للجرائم المعلوماتية بشكل عام والتي منها جريمة الدخول أو البقاء إلى نظام المعالجة

---

(1)راجع المادة (394 مكرر5) من القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم (66- 156) المؤرخ في8 يونيو 1966 يتضمن قانون العقوبات.

(2) نصت المادة (176) من قانون العقوبات الجزائري قبل التعديل- في ظل الأمر رقم (66- 156) المؤرخ في 8 يونيو 1966على أن (كل جمعيه أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد للجنايات أو ارتكابها ضد الأشخاص والأملاك تكون جناية جمعية الأشرار التي تنشأ بمجرد التصميم المشترك على العمل)، ونصت المادة (177) قبل التعديل - في ظل الأمر 66- 156 المؤرخ في 8 يونيو 1966- على أن (يعاقب بالسجن من خمس إلى عشر سنوات كل شخص يشترك في الجمعية أو الاتفاق المحدد وتكون العقوبة من عشر إلى عشرين سنه لمنظمي الجمعية أو الاتفاق أو من يباشرون فيه أي قيادات أيا كانت).أما النصوص بعد التعديل فتنص المادة (176) من القانون رقم(04 -15) المؤرخ في 10نوفمبر 2004 على أن (كل جمعية اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر أو جنحة أو أكثر معاقب عليها بخمس (5) سنوات حبساً على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل). وتنص المادة (177) من القانون (رقم04-15) المؤرخ في 10نوفمبر 2004 على أن (يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس(5) سنوات إلى عشر (10) سنوات، وبغرامة (من 500.000دج إلى 1.000.000 دج)، إذا تم الإعداد لارتكاب جنايات، وتكون العقوبة الحبس من سنتين (2) إلى خمس(5) سنوات، والغرامة من 100.000 دج إلى 500.000 دج إذا تم الإعداد لارتكاب جنح، ويعاقب منظم جمعية الأشرار أو من يباشر فيها أية قيادة كانت بالسجن من عشر سنوات (10) إلى عشرين سنة، وبغرامه من 1.000.000دج إلى 5.000.000دج).

(3) المادة (129) من ق.ع .ي رقم (12) لسنة1994.

الآلية للبيانات، وجريمة التلاعب بمعطيات الحاسوب، وجريمة تخريب النظام، إذ أن تجريم الاتفاق لا يتأتي إلا بعد أن يتم تجريم الجرائم الأساسية بالدرجة الأولى.

وجريمة الاتفاق الجنائي هي واحدة من الأحكام المشتركة التي تشترك فيها جميع الجرائم الواقعة على معطيات الحاسوب.

1- الركن الشرعي للاتفاق الجنائي

نصت المادة(394 مكرر05)على الاتفاق الجنائي حيث ورد النص (كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسداً بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقرر للجريمة ذاتها) (1).

يتضح من هذا النص أن المشرع الجزائري قد تنبه لتجريم الاتفاق الجنائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، على الرغم من أن تجريم الاتفاق الجنائي قد ورد ضمن نصوص جمعية الأشرار، وذاك دليل على خطورة جرائم المساس بأنظمة المعالجة الآلية للبيانات، وتطلب إفراد الاتفاق بشأن التحضير لارتكابها نصا مستقلاً .

كما يلاحظ بأن تطبيق هذا النص يقتصر على الجرائم المنصوص عليها في ق.ع.ج في المواد (394مكرر1 إلى394 مكرر 7) الخاصة بجرائم المساس بأنظمة المعالجة الآلية للبيانات.

ولم يتفق الفقهاء بشان تجريم الاتفاق الجنائي، فمنهم من رأى بأن الاتفاق الجنائي مجرد عزم إجرامي، بحيث لا يعتبر جريمة لأن القانون لا يعاقب على مجرد العزم، فالاتفاق الجنائي مرحلة مبكرة بالنسبة للتحضير للجريمة، إذ إنها ترد إلى المرحلة

---

(1) المادة (394 مكرر5) من القانون رقم(04 – 15)المؤرخ في 10 نوفمبر 2004 . والنص باللغة الفرنسية:
(1) Art. 394 septes_ (Loi n° 04 – 15 du10 Novembre 2004)
Quiconque Participe à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par la présente section est puni des peines prévues pour !'infraction elle-même

النفسية، بينما يعقب هذه المرحلة مرحلة التحضير للجريمة، ولو صحت خطورة الاتفاق لكان من باب أولى تجريم التحضير للجريمة[1].

بينما يرى آخرون أن الاتفاق الجنائي يعد جريمة، إلا أن تجريمه لا يعد استثناء على قاعدة عدم التجريم على مجرد العزم، وإنما على اعتبار أن الاتفاق في حد ذاته جريمة، وأن العزم الجماعي الإجرامي في الاتفاق الجنائي يظهر بمظهر مادي خارجي، لأن كل عضو يعلن عزمه إلى سائر الأعضاء، فتتحد إرادتهم على ارتكاب الجريمة، ومن ناحية ثانية فإن الاتفاق الجنائي ظاهرة خطيرة لأنه يقوم على التقاء الإرادات الإجرامية للقيام بعمل إجرامي تجعل المصالح المحروسة بنصوص القانون مهددة بالخطر، وهذا التهديد هو الأمر الذي يدعو إلى تجريم الإتفاق [2].

كما أنه لا محل للقول بأن الاتفاق الجنائي عزم إجرامي ، وبأن تجريم الاتفاق الجنائي سيجعل المجرمين يقدمون على ارتكاب جريمتهم، لأن المشرع بتجريمه للاتفاق الجنائي يكون قد وضع العقاب لأول بادرة منهم في اتفاقهم [3].

ولعل الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، هي أن هذه الجرائم تتم عادةً في إطار مجموعات، وبهدف توسيع نطاق العقوبة فقد توسع المشرع في إخضاع الأعمال التحضيرية التي تسبق البدء في التنفيذ الذي يتم في إطار اتفاق جنائي في الجرائم المعلوماتية للعقوبة، أما الأعمال التحضيرية المرتكبة من شخص منفرد فإن مثل هذه الحالات غير مشمولة بنص المادة (394 مكرر5). وتكون عقوبة الاتفاق الجنائي هي عقوبة الجريمة التي تم التحضير لها، فإذا تعددت الجرائم التي يتم التحضير لها فتكون العقوبة هي عقوبة الجريمة **الأشد**[4].

ومع أن القانون اليمني لم ينص على جريمة الاتفاق الجنائي في مجال المعلوماتية إلا أنه يمكن تطبيق نص المادة(129) التي جرمت الاتفاق الجنائي لارتكاب أي جريمة

---

(1) عبد التواب معوض، ((لاتفاق الجنائي العام في ضوء الحكم بعدم دستورية المادة 48 عقوبات مصري)) المجلة القانونية الاقتصادية، جامعة الزقازيق -كلية الحقوق، ع17، 2005، وعبد الفتاح مصطفى الصيفي، قانون العقوبات -النظرية العامة، دار الهدى، الإسكندرية، ص247، مشار إليهما في مؤلف، محمد خليفة، مرجع سابق، ص113.

(2) راجع:علي حسن الشرفي، مرجع سابق، ص312. وراجع: محمد خليفة، مرجع سابق، ص112،ص113.

(3)على حسن الشامي، جريمة الاتفاق الجنائي في قانون العقوبات المصري، مطبعة لجنة التأليف والترجمة والنشر، القاهرة، 1999، ص362.

(4) أمل قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص131.

من الجرائم الماسة بالأمن القومي للدولة على تلك الجرائم إذا ما تم اقترافها بواسطة نظم المعلوماتيـة، وعلـى المشـرع اليمنـي استحداث نـص قـانوني يعـالج هـذه المسـألة ضـمن نصوص قانونية لمواجهة جرائم المعلوماتية أسوة بالتشريع الجزائري وبعض التشريعات العربيةوالتي منها التشريع السعودي والتشريع الإماراتي[1]، والاتفاقيات الدولية[2].

2- الركن المادي للاتفاق الجنائي

يتحقق الركن المادي في الاتفـاق الجنـائي بفعل الاتفـاق وموضـوع الاتفـاق وتعـدد المتفقين .

أ- فعل الاتفاق

يتحقق فعل الاتفاق بانعقاد إرادتين أو أكثر واجتماعهما على أمر معين، والاتفـاق له مظهر مـادي ملموس مـن خـلال تعبير كل شـخص عن إرادتـه، فـالتعبير عن الإرادة يعتبر فعلا ماديًا كالقول الشفوي[3].

وإذا كان النص التقليدي في المـادة (176ع.ج) وكـذلك نـص المـادة (129 ع.ي) قد اكتفيا لتجريم الاتفاق الجنائي على مجرد توافر الإرادات، أي العنصر النفسي فحسب، فـإن الـنص الخـاص بالاتفـاق فـي جـرائم المســاس بالأنظمـة المعلوماتيـة فـي المــادة

([1]) ومن تلك التشريعات، نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية حيث تضمنت المادة(9) منه على النص على جريمة التحريض، أو المساعدة، أو الاتفاق على ارتكاب إحدى جرائم المعلوماتية المنصوص عليها في النظام، والعقوبة المقررة لها، وكذلك فقد تضمنت الماد (23) من القانون الإماراتي الاتحادي النص على جريمة التحريض أو المساعدة أو الاتفاق مع الغير على ارتكاب جريمة من جرائم المعلوماتية المنصوص عليها في القانون راجع المادة(9) من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم(م/17) المؤرخ في 1428/3/8هـ بناء على قرار مجلس الوزراء رقم (79)المؤرخ في 1428/3/7هـ وراجع المادة(23)من القانون الإماراتي الاتحادي رقم (2) لسنة 2006، بشأن مكافحة جرائم تقنية المعلومات.

([2]) ومن تلك الاتفاقيات اتفاقية بودابست 2001 المتعلقة بالإجرام المعلوماتي حيث نصت في المادة (11) على الاشتراك في ارتكاب الجرائم المعلوماتية المنصوص عليها في الاتفاقية، بضرورة تبني الدول الأطراف في الاتفاقية في تشريعاتها الداخلية عقوبة لكل اشتراك إذا تم عمدا بغرض ارتكاب إحدى جرائم المعلوماتية المشار إليها في المواد من 2-10 من الاتفاقية. وقد ورد النص بالفرنسي :

Article 11 – Tentative et complicité

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

راجع: هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 21 نوفمبر 2001، ط1، دار النهضة العربية، القاهرة، 2002، ص144. وراجع: الموقع الإلكتروني لمكافحة الجريمة الاقتصادية باللغة الفرنسية، ت.د 2008/10/26على الرابط:

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

(3) الغوثي بن ملحه،((الجريمة المنظمة في قانون العقوبات الجزائري))، مجلة كلية أصول الدين للبحوث والدراسات الإسلامية، ع3، سبتمبر2000، ص259.

(394مكرر5)ع.ج لم يكتفِ بالجانب النفسي للاتفاق الجنائي، بل إنه قد تطلبَ إضافة إلى ذلك أن يكون الاتفاق مجسداً بأفعال مادية وذلك بإضافة العبارة" وكان ذلك مجسدا بأفعال مادية". فيشترط إضافة إلى وجود العزم وتلاقي الإرادات، مرحلة أخرى هي مرحلة الأعمال التحضيرية، وهي ليست مرحلة نفسية كسابقتها، وإنما هي مرحلة مجسدة بأفعال مادية، كاقتناء برامج فيروسات، أو أي برامج اختراق، أو كتيبات تشرح من خلالها إيضاح أو اقتراف جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها بالقانون.

ب- موضوع الاتفاق

يشترط في موضوع الاتفاق أن يكون غير مشروع، وبناء على ذلك فإن الاتفاق عندما يكون موضوعه مشروعا فلا تترتب عليه جريمة.

ونص المادة (394مكرر5): الخاصة بتجريم الاتفاق الجنائي في مجال جرائم المساس بأنظمة المعالجة الآلية للمعطيات لا تجرم سوى الإعداد لجريمة الاتفاق الجنائي، ولا تتضمن تجريم الاتفاق على ارتكابها كما في نص المادة (176ق.ع.ج) التي تجرم الاتفاق على الإعداد للجريمة والاتفاق على ارتكابها، وقد يكون المشرع الجزائري وقع في السهو إذ كان يلزم أن يجرم الاتفاق على ارتكاب الجريمة كذلك، لكون مجرد الاتفاق على أعمال التحضير والإعداد يكتسب الصفة الجنائية ولو كانت الأعمال في ذاتها مشروعة[1].

ولا نتفق مع هذا الرأي لأن نص المادة (394مكرر5) قد حددت موضوع الاتفاق بالإعداد للتحضير لارتكاب جريمة أو أكثر من الجرائم المنصوص عليها، وذلك ما يوحي بأن الاتفاق على الإعداد يشمل الاتفاق على ارتكاب الجريمة، لكون من يتفقون على شراء أو تجهيز برامج يتم من خلالها ارتكاب الجريمة، إنما يعد ذلك جزء من اتفاقهم على ارتكاب الجريمة، وتؤكد ذلك الفقرة الأخيرة من النص والمتضمنة (وكان هذا التحضير مجسدًا، بفعل أو عدة أفعال مادية..)، فالأفعال المادية المشار إليها تدل على الاتفاق المسبق لارتكاب الجريمة، وذلك ما تضمنه نص المادة (176) ق.ع حيث تضمن عبارة " الاتفاق بغرض الإعداد لجناية أو جنحة".

([1]) محمد خليفة، مرجع سابق، ص114.

ويجب أن يكون للاتفاق هدف إجرامي من ذو البداية، فإذا لم يوجد هدف فلا تتحقق جريمة المساس بالأنظمة المعلوماتية، مثل الاتفاق الذي يقوم على تأسيس ناد للتسلية[1].

ج- تعدد الجناة

تتطلب جريمة الاتفاق في ارتكاب أية جريمة من الجرائم المعلوماتية المنصوص عليها في المادة (394 مكرر5)من ق.ع.ج، تعددا ضروريا للجناة، بحيث يكون الحد الأدنى للتعداد شخصين، بينما لا يرد قيد في القانون على الحد الأعلى للعدد.

فإذا تحققت الشروط المذكورة فقد تحققت الجريمة، و لا يهم بعد ذلك أن يكون أعضاء الاتفاق جماعة أم شخصاً معنوياً، كما لا يهم أن يكون أعضاء الاتفاق يعرف بعضهم بعضاً أم لا، والمهم هو أن يتم الاتفاق بين شخصين فأكثر، بأي طريقة كانت.

3- الركن المعنوي

جريمة الاتفاق في جرائم المعلوماتية يجب أن يتوافر فيها القصد الجنائي العام بعنصرية العلم والإرادة.

فيجب أن يحيط الجاني علمه بكل العناصر اللازمة لوجود الجريمة، كما حددها القانون، بالإضافة إلى كل واقعة أو تكييف ذا أهمية في بيان الجريمة، ويتحدد ذلك بالرجوع إلى كل حالة على حدة وإلى النص القانوني الخاص بها[2].

ويجب كذلك أن يعلم كل عضو في الاتفاق على ارتكاب جريمة معلوماتية بماهية الفعل أو الأفعال التي يقدم على ارتكابها مع غيره، ولابد أن يعلم بأنه يقوم مع غيره بارتكاب إحدى جرائم المعلوماتية – الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات، أو التلاعب في لمعطيات المخزنة بنظام المعالجة الآلية للمعطيات، أو التعامل مع المعطيات الغير شرعية وغيرها من الجرائم المنصوص عليها في ق.ع .ج.

ويترتب على ما سبق انتفاء العلم في حالة ما إذا كان الشخص- طرف الاتفاق- يعتقد أن الاتفاق تم للقيام بالاتجار ببرامج أو معطيات مشروعة، واتضح له بعد ذلك عدم صحة ما يعتقد[3].

---

(1) آمل قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص131.
(2) راجع: حسني الجندي، شرح قانون العقوبات اليمني، دار النهضة العربية، القاهرة،1990،ص385.
(3) راجع: آمل قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص132.

كما يجب لقيام جريمة الاتفاق الجنائي أن تتحقق الإرادة بجانب العلم، ولكي يعتد بالإرادة في جريمة الاتفاق الجنائي في الجرائم المعلوماتية، لابد أن تنعقد إرادتان فأكثر لارتكاب نشاط إجرامي وهو العمل التحضيري، ولابد أن تنصرف تلك الإرادات لاقتراف إحدى جرائم المعلوماتية.

4- العقوبات

عقوبة الاتفاق الجنائي وفقا لنص المادة (394مكرر5) هي نفس العقوبة المقررة للجريمة ذاتها، بخلاف بعض التشريعات التي عاقبت على الاتفاق في جرائم المعلوماتية بما لا يتجاوز عقوبة الجريمة ذاتها بشرط تحقق الجريمة محل الاتفاق، فإذا لم تتحقق الجريمة فتكون العقوبة بما لا يتجاوز نصف عقوبة الجريمة الأصلية.

وبعض التشريعات لا تعاقب على الاتفاق إلا إذا تحققت الجريمة وتكون العقوبة هي عقوبة الجريمة الأساسية[1].

وبناء على ذلك فعقوبة الاتفاق على الإعداد لارتكاب جريمة الدخول أو البقاء هي نفسها عقوبة جريمة الدخول والبقاء، والأمر نفسه بالنسبة لباقي الجرائم الخاصة بالمساس بأنظمة المعالجة الآلية للمعطيات.

كذلك فإن عقوبة الاتفاق الجنائي في الجرائم الماسة بالأمن القومي للدولة وفقا لـ ق.ج.ع.ي هي نفس عقوبة الجريمة ذاتها وقد تم إيضاح عقوبات تلك الجرائم أثناء تناول الجرائم الماسة بالأمن القومي للدولة.

([1]) نصت المادة 9 من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم(م/17) المؤرخ في7/ 3/ 1428 هـ، الموافق 26/ 3/ 2007 بناء على قرار مجلس الوزراء رقم (79) على أن: (يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية).

أما القانون الإماراتي الاتحادي رقم (2) لسنة 2006 ، بشأن مكافحة جرائم تقنية المعلومات فلا يعاقب على جريمة الاتفاق إلا إذا تحققت الجريمة محل الاتفاق وتكون عقوبتها هي عقوبة الجريمة ذاتها، وذلك بموجب نص المادة (23) والذي نص على أن (كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة للجريمة ذاتها).

المطلب الثاني

الشروع في مجال الجريمة المعلوماتية

الشروع في الشيء هو البدء في القيام به، والشروع في الجريمة ينصرف إلى البدء في تنفيذها [1].

ويشترط في الشروع عدم تحقق النتيجة الإجرامية لأسباب خارجة عن إرادة الجاني، وبالتالي فقد يقوم الجاني بتنفيذ النشاط الذي بواسطته تتحقق النتيجة، إلا أن ذلك النشاط يتوقف بسبب خارج عن إرادة الجاني، كتدخل شخص أخر، وتعرف هذه الحالة بالجريمة الموقوفة، وفي الجريمة المعلوماتية فقد يقوم الجاني بنشاطه المتمثل في الدخول إلى نظام معلوماتي إلا أن ذلك النشاط لا يكتمل بسبب تدخل شخص أخر أوقف ذلك النشاط، وقد يستكمل الجاني نشاطه إلا أن النتيجة لا تتحقق لسبب كان يجهله، ومثال ذلك في الجريمة المعلوماتية من يقوم باستخدام برنامج للدخول إلى النظام والتلاعب بالبيانات، ويستطيع تحقيق الدخول لا كنه لا يستطيع تحقيق الجريمة الأخرى لخلل في البرنامج، وبالتالي تتحقق جريمة الدخول، وجريمة الشروع في التلاعب بالمعطيات، وفي هذه الحالة تسمى الجريمة بالجريمة الخائبة.

1- الركن الشرعي

أدرك المشرع الجزائري خطورة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فجرم الشروع في ارتكاب تلك الجرائم مع أنها جنح ،حيث إن الأصل في التجريم بالنسبة للشروع في الجنح لا يكون إلا بنص جنائي .

وقد نصت المادة (30)ق.ع.ج على جريمة الشروع بشكل عام تحت عنوان المحاولة، حيث نصت على (كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي إلى ارتكابها، تعتبر كالجناية نفسها إذا لم توقف أو يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها، حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها) [2].

---

(1) علي حسن الشرفي، مرجع سابق، ص254.

(2) المادة (30) من الأمر رقم(66-156) المؤرخ في 18 صفر 1386 هـ الموافق 8 يونيو سنة 1966المتضمن قانون العقوبات المُعَدَلْ والمُتَمَمْ .راجع، فضل العيش، قانون العقوبات، وفقا للتعديلات الأخيرة 2006، منشورات بغدادي ،الجزائر،2007، ص 172.

كما نصت المادة (394 مكرر7) على جريمة الشروع في مجال المعلوماتية وذلك بأن (يعاقب على الشروع بارتكاب الجنح المنصوص عليها في هذا القسم- السابع من ق.ع.ج- بالعقوبات المقررة للجنحة ذاتها)[1] .

وتجريم الشروع وفقا للنص الأخير يهدف إلى توسيع نطاق العقوبة للجرائم المعلوماتية، لتشمل اكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، حتى إنه قد سوى بين الشروع والجريمة التامة من حيث العقوبة.

وقد تبنى فكرة الشروع في الاتفاق الجنائي مع أن بعض التشريعات لم تتبنى ذلك، ومنها التشريع الفرنسي، كون ذلك يؤدي إلى المساس بالنظرية العامة في القانون الجنائي، وهي العقاب على مجرد التحضير أو التفكير في الجريمة، وكان ذلك بهدف توسيع نطاق العقوبة للجرائم التي تتم من خلال الاتفاق الجنائي في الجرائم المعلوماتية[2].

كما نص ق.ج.ع.ي على جريمة الشروع في المواد (18، 19)، حيث تم تعريف الشروع وبيان أركانه من خلال نص المادة (18) بأنه: (البدء في تنفيذ فعل بقصد ارتكاب جريمة إذا أوقف سلوك الفاعل، أو خاب أثره، لسبب لا دخل لإرادته فيه، ولو استحال تحقق الجريمة التي قصد الفاعل ارتكابها لقصور الوسيلة المستعملة، أو لتخلف موضوع الجريمة، أو لعدم وجود المجني عليه)[3].

كما نصت المادة (19) على جريمة الشروع بقولها (يعاقب على الشروع دائما، ولا تزيد العقوبة عن نصف الحد الأقصى المقرر للجريمة التامة، إلا إذا نص القانون على خلاف ذلك، وإذا كانت عقوبة الجريمة التامة هي الإعدام، تكون عقوبة الشروع الحبس الذي لا يزيد على عشر سنوات وتسري على الشروع الأحكام الخاصة بالعقوبات التكميلية المقررة للجريمة التامة)[4]

---

(1) المادة (394 مكرر7) من القانون رقم(04 – 15) المؤرخ في 10 نوفمبر 2004 المُتَمِمْ لقانون العقوبات الجزائري. ونص المادة بالفرنسي

Art. 394 noniés (Loi n° 04 – 15 du10 novembre 2004) La tentative des délits prévus à la présente section est punie des mêmes peines pour le délit lui- même.

(2) محمد خليفة، مرجع سابق ، ص118.

(3) المادة (18) من القانون اليمني (رقم 12 لسنة 1994) بشأن الجرائم والعقوبات.

(4) المادة (19) ع.ي.

ويلاحظ من خلال نصوص القانون اليمني عدم تضمينها تجريم الشروع في الجريمة المعلوماتية، بخلاف بعض القوانين ومنها الجزائري و السعودي[1]، والاتفاقيات الدولية ومنها اتفاقية بودابست[2].

2- الركن المادي

يقوم الركن المادي في جريمة الشروع وفقا للنظرية المادية باقتراف الفعل أو الأفعال المادية المكونة للجريمة، وبالتالي فإنه وفقا لهذه النظرية تخرج الأفعال التحضيرية السابقة على اقتراف الجريمة من جرائم الشروع.

بينما يقوم وفقا للنظرية الشخصية بالنظر إلى شخص الجاني ونفسيته، فيقوم الشروع إذا قام الجاني بوضع كل ما أعده من وسائل موضع التنفيذ، حتى لو كان من الأعمال التحضيرية[3].

ويرجح البعض المذهب المادي على المذهب الشخصي، لأنه لا يعاقب على الشروع إلا إذا وضع الجاني يده على الفعل المحقق للنتيجة، وإلا فإنه سيؤاخذ على مجرد النية، وبالتالي فيستبعد من الشروع مجرد التفكير فيها أو التصميم عليها أو إعداد العدة لها قبل البدء في التنفيذ[4]. وقد تبنت بعض القوانين هذا الاتجاه[5].

([1]) تضمنت المادة (10) من نظام مكافحة الجرائم المعلوماتية السعودي، النص على جريمة الشروع في الجرائم المعلوماتية المنصوص عليها في النظام، وحددت عقوبتها بنصف عقوبة الحد الأعلى للجريمة المعلوماتية.

([2]) تضمنت الفقرة(2) من المادة (11) من اتفاقية بودابست، إلزام الدول الأطراف في الاتفاقية بتبني الإجراءات التشريعية أو أي إجراءات أخرى لتجريم كل شروع عمدي لارتكاب إحدى الجرائم المعلوماتية المنصوص عليها في الاتفاقية، حيث ورد النص بالفرنسي:

Article 11 – Tentative et complicité

2 - Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

راجع: هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 21 نوفمبر 2001، مرجع سابق، ص144. وراجع: الموقع الإلكتروني لمكافحة الجريمة الاقتصادية، 10/26/ مرجع سابق 2008على الرابط:

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

([3]) راجع: علي حسن الشرفي، مرجع سابق، ص265. وراجع أيضا: سعيد حميدة: الشروع أو المحاولة في قانون العقوبات الجزائري، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 1979، ص75.

([4]) على حسن الشرفي، مرجع سابق، ص255.

([5]) ومن تلك القوانين قانون العقوبات القطري رقم (11) لسنة 2004 حيث نصت المادة (28) الفقرة الثانية(ولا يعتبر شروعا في جناية أو جنحة مجرد العزم على ارتكابها، ولا الأعمال التحضيرية لها، ما لم ينص القانون على خلاف ذلك)، ت.د.2008/10/28 على الرابط :

http://62.215.234.226/MojPortalPublic/LawAsPDF.aspx?opt&country=3&LawID=2597

فالركن المادي في جريمة الشروع يقوم على الأفعال المادية التنفيذية التي كانت ستؤدي إلى تحقيق النتيجة الإجرامية لولا تدخل عوامل خارجية حالت دون وقوعها لأسباب خارجة عن إرادة الجاني.

وفي الجرائم المعلوماتية يقوم الركن المادي على ذات الأفعال التي تقوم بها الجريمة، ففي جريمة الدخول والبقاء في نظام المعالجة الآلية للمعطيات يقوم الركن المادي على الشروع في فعل الدخول وفعل البقاء، إلا أن الجريمة لا تتحقق لأسباب خارجة عن إرادة الجاني، وهكذا في بقية الجرائم وفقا لما سيتم إيضاحه أثناء تناول كل جريمة على حدة.

فقد يقوم الجاني بتثبيت البرنامج الذي يستطيع من خلاله الدخول إلى النظام، أو اقتراف أي جريمة من الجرائم المعلوماتية المنصوص عليها، ومن ثم البدء بالأفعال التي تؤدي إلى الاختراق وارتكاب أي من جرائم المعلوماتية ومنها فتح شبكة الاتصالات والبدء في الاتصال بالنظام المستهدف، إلا أن تدخل أسباب وعوامل أخرى حالت دون تحقق ذلك كانطفاء التيار الكهربائي.

3- .الركن المعنوي

يتحقق الركن المعنوي في الشروع بتوافر القصد الجنائي الذي تتطلبه الجريمة التامة(1)، حيث يتطلب توافر عنصري العلم والإرادة.

ويشترط لتحقق عنصر العلم أن يكون الجاني عالما بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة واستكمال عناصرها يتعين أن يكون الجاني عالما بها(2).

وفي مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ينبغي أن يكون الجاني عالما بكل واقعة ذات أهمية قانونية تدخل في تكوين الجريمة، سواء تمثلت تلك الجريمة بجريمة الدخول والبقاء غير المشروع إلى نظام المعالجة الآلية للمعطيات، أو جريمة التلاعب بمعطيات الحاسوب، أو جريمة التعامل بالمعطيات غير الشرعية الناتجة أو التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية المنصوص عليها في ق.ع .ج.

---

(1) علي حسن الشرفي، مرجع سابق، ص268.
(2) نائلة عادل محمد فريد فورة، مرجع سابق، ص365.

ففي جريمة الدخول غير المشروع – على سبيل المثال - يجب أن يعلم الجاني أنه يقوم بمحاولة الدخول غير المشروع إلى جهاز الحاسب الآلي غير المصرح له بالدخول إلى نظامه، وهكذا بالنسبة إلى بقية الجرائم.

وإذا ما توافر عنصر العلم على النحو السابق فإنه يتعين توافر العنصر الثاني من عناصر القصد الجنائي، وهو الإرادة التي بموجبها يتطلب أن تتجه تلك الإرادة لتحقيق النتيجة، وهي الدخول، إلا أن النتيجة لا تتحقق لعوامل خارجة عن إرادة الجاني.

و قد يثار تساؤل حول سبب تكرار النص على الشروع بالنسبة لجريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات، حيث أن المادة(394مكرر) بعد أن نصت على جريمة الدخول جرمت المحاولة بقولها (أو يحاول ذلك)، وكذلك المادة(394)مكرر7) التي تضمنت الشروع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بما فيها جريمة الدخول غير المشروع أو المحاولة، وتجريم محاولة الدخول، والنص بعد ذلك على تجريم الشروع يفيد بوجود شروع داخل الشروع، فهل هذا التكرار يجعل من لفظ (أو يحاول ذلك في جريمة الدخول) يختلف عن الشروع، بمعنى آخر هل المحاولة لارتكاب الجريمة تختلف عن الشروع؟

ونجيب على ذلك التساؤل بأن المحاولة لا تختلف عن الشروع في النصين السابقين، بدليل أن المشرع الجزائري في نص أخر وهو نص المادة (30)ع. قد نص على الشروع بعنوان المحاولة، مما يجعل مصطلحي المحاولة والشروع تحمل معنى واحد، وبالتالي فإن تكرار اللفظ في جريمة الدخول يجد له تفسيرا بأهمية هذه الجريمة، لكونها الجريمة الأولى التي يمكن أن تكون بمثابة البوابة لارتكاب اغلب الجرائم المعلوماتية، وكان يستحسن عدم شمول نص المادة (394 مكرر) لفظ المحاولة والاكتفاء بنص المادة(394 مكرر7) المتضمن تجريم الشروع في جميع جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القانون[1].

4- العقوبات

تختلف عقوبة الشروع في الجرائم المعلوماتية المنصوص عليها في ق.ع.ج.عن عقوبة جريمة الشروع في ق.ج.ع.ي.

([1]) راجع: المادة (394 مكرر) والمادة(394 مكرر7) من

فبينما يعاقب القانون الجزائري على جريمة الشروع بعقوبة الجريمة التامة فإن القانون اليمني يعاقب عليها بنصف عقوبة الجريمة الأصلية [1] باستثناء الجرائم الماسة بالأمن القومي للدولة التي يعاقب فيها على الشروع بنفس عقوبة الجريمة التامة.

كذلك فإن بعض القوانين تكتفي بنصف عقوبة الجريمة التامة ومنها قانون العقوبات القطري، ونظام مكافحة الجرائم المعلوماتية السعودي [2].

المطلب الثالث

الجرائم المعلوماتية المرتكبة ضد المؤسسات والهيئات ألعامة

لم تقتصر الحماية الجنائية على الاعتداءات الموجهة لمؤسسات ألدولة والهيئات الخاضعة للقانون العام وفقا للقوانين التقليدية فحسب، بل إن تلك الحماية قد تضمنتها نصوص خاصة في أغلب القوانين، وعلى وجه الخصوص تلك التي ترتكب بواسطة المعلوماتية، نظرا للتعاملات التي فرضت على تلك المؤسسات بسبب التطور التكنولوجي الذي جعل تلك التعاملات تسيرها أنظمة آلية، حيث تم تشديد العقوبات في مواجهة هذا النوع من الإجرام .

1- الركن الشرعي

نصت المادة (394 مكرر3)ع.ج على تجريم الدخول إلى بعض الأنظمة الخاصة بالدفاع الوطني، أو المؤسسات والهيئات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد، حيث ورد النص كالتالي: (تضاعف العقوبات المنصوص عليها في هذا

([1]) راجع: المادة (30) من ق.ج.ع.ي رقم(12) لسنة 1994.

([2]) يعاقب نظام مكافحة الجرائم المعلوماتية السعودي على جريمة الشروع في جرائم المعلوماتية بنصف العقوبة المقررة للجريمة التامة وفقا لنص المادة العاشرة حيث نصت على أن (يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة). وكذلك قانون العقوبات القطري رقم(11)لسنة 2004 في الفصل الخامس الخاص بجرائم الحاسب الآلي المواد من 370: 387- حيث نصت عليها المادة 387 (يعاقب على الشروع في الجنح المنصوص عليها في هذا الفصل، بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة التامة).

القسم، إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد) [1].

وبناء على ما ورد في النص فإن أي فعل يستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، إذا تحققت به إحدى الجرائم المنصوص عليها في القسم السابع مكرر من ق.ع.ج، سواء كانت جريمة الدخول أو البقاء إلى أنظمة المعالجة الآلية لنظم تلك المؤسسات أو الهيئات، أو جريمة إتلاف الأنظمة، أو غير ذلك من الاعتداءات الموجهة ضد الأنظمة، أو المعطيات المدرجة بتلك النظم، فإنه يقع تحت طائلة المساءلة وفقا لنص المادة (394 مكر 3). فكثير من التشريعات عند تجريمها العدوان على أنظمة ومعطيات الحاسوب، تولي الاهتمام الأكبر للأنظمة والمعطيات التي تتبع الدولة أو إحدى الموسوسات التابعة لها.

وبالنسبة للقانون اليمني فما زال لم يتضمن نصا قانونيا يتناول تجريم الاعتداءات المعلوماتية على نظم مؤسسات الدفاع الوطني، والمؤسسات والهيئات الخاضعة للقانون العام، ويتعامل معها وفقا للنصوص التقليدية بقانون العقوبات.

2- الركن المادي

الركن المادي للجرائم المعلوماتية التي يستهدف من خلالها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، يتمثل بالأفعال والنتائج الخاصة بكل جريمة على حدة، وسيتم إيضاحها أثناء تناول الركن المادي لجريمة الدخول والبقاء إلى نظام المعالجة الآلية للمعطيات، وجريمة التلاعب بالمعطيات، وجريمة التعامل مع معطيات غير شرعية متحصلة من جريمة، أو يمكن أن ترتكب بها جريمة معلوماتية

---

(1) ونص المادة بالفرنسي :

Art. 394 quinquiés,- (Loi n° 04 – 15 du10 novembre 2004) Les peines Prévues par la présente section sont portées au double lorsque l'infraction porte atteinte à la défense nationale aux organismes ou établissements de droits public , sans préjudice de l'application des peines plus sévères .

كما تجرم بعض التشريعات تلك الأفعال التي تمس الأنظمة الآلية للمعطيات إذا استهدفت تلك الأفعال أنظمة معينه، ومن ذلك التشريع الأمريكي "قانون الغش في مجال البرمجة في الولايات المتحدة الأمريكية Computer fraud and Abuse Act" والذي يجرم الدخول إلى كمبيوترات بعض الجهات مثل وزارتي الدفاع والخارجية، كما تقع الجريمة إذا كان مسموحا بالدخول إلى تلك الأجهزة وحدث تجوز لها. راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص323.

وغيرها من الجرائم التي سيتم إيضاح الأحكام الخاصة بكل منها على حدة، وذلك تفاديا لعدم التكرار.

والفارق بين الركن المادي في هذه الجريمة والركن المادي لكل جريمة على حدة هي أن تلك الأفعال التي يتم بواسطتها ارتكاب جريمة معلوماتية في هذه الجريمة تكون موجهة ضد مؤسسات الدولة والهيئات الخاضعة للقانون العام.

3- الركن المعنوي

الركن المعنوي للجرائم المعلوماتية التي تستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام لا يختلف عن الركن المعنوي الذي سيتم إيضاحه أثناء تناول كل جريمة على حدة، والمتمثل بالقصد الجنائي العام بعنصرية العلم والإرادة، والمتطلب تحققه في اغلب الجرائم باستثناء جريمة الدخول أو البقاء في صورتيهما المشددة التي تطلب المشرع فيهما القصد الجنائي الخاص إلى جانب القصد الجنائي العام.

والجديد في الجرائم المعلوماتية التي ترتكب ضد الدفاع الوطني، والمؤسسات والهيئات الخاضعة للقانون العام بجانب العلم بكل عناصر وأركان الجريمة، لابد أن يكون الجاني عالما بأنه يرتكب جريمة معلوماتية ضد مؤسسة أوجهه عامة، ويقدم على اقتراف تلك الجريمة بإرادته، قاصدا إحداث النتيجة المتمثلة بالخطر في جرائم الخطر، وبالضرر في جرائم الضرر.

4- العقوبات

كما أن الجرائم المعلوماتية تشترك في بعض الأحكام المتعلقة بالتجريم، فهي كذلك تشترك في بعض الأحكام المتعلقة بالعقوبة، ومن ذلك تشديد عقوبة الاعتداء على الأنظمة والمعطيات المتعلقة بالدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام عن غيرها من الجهات والأشخاص نظرا لحساسية المعطيات التي تتعامل بها تلك الموسوسات التي من شأنها حماية أمن وسلامة البلاد .

ففي حالة ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذا استهدفت تلك الجريمة مؤسسة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام، فإنه يتم مضاعفة العقوبة عما هي عليه بالنسبة للجرائم التي تستهدف الأفراد وأشخاص القانون الخاص، وبالتالي فإن المسألة مقيدة بالعقوبات المنصوص عليها لكل جريمة على حدة، ومضاعفتها وبيان ذلك لكل جريمة كما يلي:

أ- عقوبة جريمة الدخول والبقاء في أنظمة مؤسسة الدفاع الوطني والمؤسسات والهيئات الخاضعة للقانون العام

حيث أن جريمة الدخول والبقاء لها صورتين ولكل صورة عقوبة، فهي تختلف في صورتها العادية عندما تقتصر النتيجة على مجرد الدخول والبقاء إلى أنظمة مؤسسات الدفاع الوطني والهيئات التي تخضع للقانون العام عنها في صورتها المشددة عندما ينتج عنها حذف أو تعديل المعطيات أو تخريب نظم تلك المؤسسات والهيئات:

1) العقوبات البسيطة

في هذه الحالة تتضاعف العقوبة لتصبح "الحبس من ستة (6) أشهر إلى سنتين(2) والغرامة من مائة ألف(100.000دج) إلى مائتي ألف (200.000دج)، بعد أن كانت عقوبة الجريمة حينما تستهدف أنظمة الأشخاص أو الأفراد العاديين هي الحبس من ثلاثة (3) أشهر إلى سنة (1) والغرامة من (50.000 دج) إلى (100.000 دج).

2) العقوبات المشددة

- إذا ترتب على جريمة الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة: فإن العقوبة تصبح (الحبس من سنة (1)إلى أربع(4) سنوات، والغرامة من مائتي ألف (200.000دج) إلى أربعمائة (400.000دج). وليس كما يرى البعض في الغرامة من (100.00 دج إلى 200.000 دج)[1].ففي هذه الحالة تم مضاعفة العقوبة مرتين الأولى: إذا ارتكبت ضد الأشخاص والجهات الخاضعة للقانون الخاص، وفقا لنص المادة(394 مكرر)**والثانية**: إذا تم ارتكابها ضد المؤسسات والجهات الخاضعة للقانون العام، وفقا لنص المادة(394 مكرر 3) حيث نصت على أن:

([1]) محمد خليفة ، مرجع سابق، ص129.

(تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات أشد)[1].

- إذا ترتب على جريمة الدخول أو البقاء تخريب نظام اشتغال المنظومة: فتصبح عقوبة الحبس من سنة (1) إلى أربع (4)سنوات، والغرامة من مائة ألف(100.000دج) إلى ثلاثة ألف (300.000دج)بعد أن كانت الحبس من ستة أشهر (6) إلى سنتين (2) والغرامة من خمسين ألفاً (50.000 دج) إلى مائة وخمسين ألفا(150.000دج).

ب- عقوبة جريمة التلاعب بالمعطيات

تضاعف العقوبة لكل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال، أو عدل بطريق الغش المعطيات التي يتضمنها نظام المعالجة الآلية التابع لمؤسسة الدفاع الوطني، أو الهيئات الخاضعة للقانون العام، حيث تصبح عقوبة الحبس من سنة(1) إلى ست(6)سنوات، والغرامة من مليون (1000.000دج)إلى أربعة ملايين (4000.000دج)، وذلك بعد أن كانت العقوبة لمرتكبي نفس الجريمة في حالة اقترافها في مواجهة أشخاص القانون الخاص هي الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من (500.000د.ج) إلى (2.000.000 د.ج).

ج- عقوبة جريمة التعامل في المعطيات غير المشروعة[2]

وفي هذه الحالة وبموجب نص المادة (394مكرر3) فان العقوبة تصبح الحبس من أربعة أشهر (4) إلى ست سنوات(6) ، والغرامة من مليونين(2.000.000 د.ج) إلى عشرة ملايين (10.000.000د.ج)، بعد أن كانت وفق نص المادة

([1]) راجع المادة (394 مكرر) والمادة (394 مكرر3) من القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004 المُعّدِلِ المُتَمِمْ لقانون العقوبات الجزائري.

([2]) وتتمثل هذه الجرائم في نوعين فهي إما ناتجة عن إحدى الجرائم المعلوماتية المنصوص عليها في ق.ع.ج ، أو يمكن أن ترتكب بها إحدى الجرائم المعلوماتية المنصوص عليها (وسائل أو معطيات أو برامج)وتتمثل في:

- تصميم، أو بحث، أو تجميع، أو توفير، أو نشر، أو الاتجار، في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم السابع من ق.ع.ج والخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.
- حيازة، أو إفشاء، أو نشر، أو استعمال، لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص في القسم المشار إليه.

(394مكرر)هي الحبس من شهرين (2) إلى ثلاث(3) سنوات والغرامة من مليون (1.000.000 د.ج) إلى خمسة مليون (5.000.000 د.ج).[1]

د- عقوبة الجرائم المرتكبة من شخص معنوي ضد مؤسسة الدفاع الوطني ومؤسسات وهيئات القانون العام

كما أن الجرائم المعلوماتية ضد مؤسسات وأشخاص القانون العام يمكن ارتكابها من قبل الشخص الطبيعي، فكذلك يمكن ارتكابها من قبل الشخص المعنوي، والعقوبة التي يمكن تطبيقها على الشخص المعنوي في حالة ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ضد إحدى الجهات العامة، هي عقوبة الغرامة.

ولكون العقوبة قد شددت إلى خمسة أضعاف بالنسبة للجريمة المعلوماتية المرتكبة من قبل الشخص المعنوي إذا استهدفت الأفراد وأشخاص القانون الخاص[2]، بالإضافة إلى أن العقوبة قد تم مضاعفتها بالنسبة للجرائم المرتكبة ضد مؤسسات وأشخاص القانون العام[3]، فإن عقوبة الجريمة المرتكبة من الشخص المعنوي ضد مؤسسات وهيئات القانون العام تكون قد ضوعفت مرتين، الأولى خمسة أضعاف باعتبار أن الجريمة مرتكبة ضد شخص طبيعي والثاني مرتين أو ضعفين باعتبار أن المجني عليه أحد أشخاص القانون العام، بمعنى أخر فإن العقوبة تضاعف إلى عشرة أضعاف ما هو مقرر على الشخص العادي لتصبح على النحو التالي:

1) عقوبة جريمة الدخول والبقاء

تكون عقوبة جريمة الدخول أو البقاء المرتكبة من الشخص المعنوي ضد إحدى جهات القانون العام في صورتها العادية – المجردة- هي (الغرامة من 50.000×10=500.000دج خمسمائة ألف دينار جزائري إلى 100.000×10=1000.000دج) مليون دينار جزائري[4].

و تكون عقوبة جريمة الدخول أو البقاء المرتكبة من الشخص المعنوي ضد إحدى الجهات العامة في صورتها ألمشددة وفقا لأمرين:

---

(1) المواد (394 مكرر2) و(394 مكرر3) من (القانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004).
(2) راجع: الماد (394 مكرر4) من نفس القانون.
(3) المادة 394 مكرر3 من القانون نفسه.
(4) راجع المواد (394 مكرر، و 394 مكرر3، و394 مكرر4) من القانون رقم(04 – 15) المؤرخ في 10 نوفمبر 2004 المُعَدِّلْ والمُتَمِمْ لقانون العقوبات الجزائري.

ففي حالة أن يترتب على الجريمة تغيير أو حذف لمعطيات المنظومة تكون العقوبة هي الغرامة من (50.000×10× 2=1.000.000دج مليون دينار جزائري- إلى 100.000×10×2=2.000.000دج مليوني دينار جزائري)[1].

أما في حال أن يترتب على الجريمة تخريب نظام اشتغال المنظومة فتكون عقوبة الغرامة هي (من 50.000×5×2=500.000دج خمسمائة ألف دينار إلى 150.000× 5×2= 1.500.000دج مليون وخمسمائة ألف دينار)[2].

2) عقوبة جرائم التلاعب بالمعطيات المخزنة في أنظمة المعالجة الآلية لإحدى الجهات العامة المرتكبة من قبل الشخص المعنوي

تتراوح عقوبة الغرامة لجريمة التلاعب بالمعطيات والمرتكبة من قبل الشخص المعنوي ضد إحدى الجهات العامة (من 500.000 ×10 =5.000.000 د.ج خمسة ملايين **إلى** 2.000.000×5×2=2.000.000د.ج عشرين مليون دينار جزائري)[3].

3) عقوبة جرائم التعامل في معطيات غير مشروعة

تكون عقوبة جريمة التعامل في معطيات غير شرعية ناتجة، أو يمكن أن ترتكب بها إحدى الجرائم المعلوماتية المنصوص عليها في ق.ع.ج عندما ترتكب من قبل الشخص المعنوي، وتستهدف مؤسسات وأشخاص القانون العام هي الغرامة (من 1.000.000×10=10.000.000دج "عشره ملايين" إلى 5.000.000 ×10 =50.000.000دج "خمسين مليون دينار).

ويلاحظ من خلال الغرامات المشار إليها وعلى وجه الخصوص الغرامة التي يتحملها الشخص المعنوي في حالة ارتكاب أي من تلك الجرائم السابقة، أنها كبيرة جدا، وقد تؤدي إلى إفلاس الشخصية المعنوية وإرهاقها ماديا، وعلى وجه الخصوص الشركاء المساهمون في الشخصية المعنوية، لذلك نرى إعادة النظر في تشديد عقوبة الغرامة للشخص المعنوي بالدرجة الأولى، وكذلك الطبيعي بما يتناسب مع تحقيق الهدف من إقرار العقوبة، وبما يتناسب مع الذمة المالية للأشخاص.

---

(1) راجع:ألفقره الثانية من المادة (394 ، والمواد 394 مكرر3، و394 مكرر4) من القانون رقم(04 – 15) المؤرخ في 10 نوفمبر 2004 المُعَدِّلْ والمُتَمِمْ لقانون العقوبات الجزائري.
(2) راجع الفقرة الثالثة من المادة (394 مكرر،والمواد 394 مكرر3، و394 مكرر4) من نفس القانون.
(3) المواد (394 مكرر2 ،و394 مكرر3،و394 مكرر4) من نفس القانون.

كما يلاحظ على العقوبات المطبقة على الجرائم التي تستهدف الدفاع الوطني أو المؤسسات والهيئات الخاضعة للقانون العام بأنه متى تعارضت تلك العقوبات مع عقوبات اشد فتطبق العقوبات الأشد.

المطلب الرابع

الجريمة المعلوماتية المرتكبة من الشخص المعنوي

الشخصية المعنوية يمكن أن ترتكب إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات عن طريق ممثليها، أي من لهم الصفة في تمثيل الشخص المعنوي أمام الغير.

وقد نص قانون العقوبات الجزائري على عقوبة الشخص المعنوي في حالة ارتكاب إحدى الجرائم المعلوماتية المنصوص عليها في القانون حيث شدد العقوبة ليجعلها تساوي خمس مرات عقوبة الشخص الطبيعي للجريمة ذاتها.

وبما أنه قد سبق إيضاح عقوبة الجرائم المرتكبة ضد أشخاص القانون العام، فيتبقى لنا إيضاح عقوبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي يمكن أن ترتكب من قبل الشخصية المعنوية، وقبل ذلك سنتناول بنوع من الإيجاز أركان الجرائم المعلوماتية التي تقترف من قبل الشخصية المعنوية، وسوف يتم إيضاح أركان كل جريمة تفصيلا أثناء تناول كل جريمة على حده.

1- الركن الشرعي

نصت على عقوبة الجرائم المعلوماتية المرتكبة من قبل الشخص المعنوي المادة (394مكرر4)ع.ج بقولها: (يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5)مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي)[1].

ولم يتضمن القانون اليمني مثل هذا النص، باعتبار أنه مازال لم يتضمن النصوص القانونية التي تجرم ارتكاب جرائم المعلوماتية بشكل عام، وعلى وجه الخصوص

([1]) ونص المادة بالفرنسي:
(Art. 394 sixties .- (Loi n° 04 – 15 du10 novembre 2004) La personne morale qui a commis une infraction prévue par la présente section est punie d'une amende qui équivaut à cinq (5) fois le maximum de l'amende prévue la personne physique).

المستحثة منها، والمرتكبة من قبل الشخص الطبيعي، فهو كذلك ومن باب أولى لم يتضمن نصوصا صريحة تجرم ارتكاب جرائم المعلوماتية المرتكبة من قبل الشخص المعنوي، إذ أن التجريم في الحالة الثانية يكون لاحقا أو متزامنا على الأقل للتجريم في الحالة الأولى.

وقد سار التشريع الجزائري بذلك على ضوء ما تضمنته الاتفاقية الدولية للإجرام المعلوماتي[1].

([1]) نصت المادة (12) من اتفاقية بودابست على مسؤولية الأشخاص المعنوية وحثت الدول الأعضاء على العمل بما ورد بالنص حيث ورد النص على النحو التالي :

- يجب على كل طرف أن يتخذ الإجراءات التشريعية، أو أي إجراءات يرى أنها ضرورية من أجل اعتبار الأشخاص المعنوية مسؤولة عن الجرائم المشار إليها في الاتفاقية الحالية إذا ارتكبت لمصلحتها عن طريق شخص طبيعي آخر، يتصرف بشكل فردي، أو بوصفه عضوا في مؤسسة الشخص المعنوي، ويمارس سلطة القيادة في داخلها بناء على القواعد التالية، سلطة تمثيل الشخص المعنوي، أو سلطة اتخاذ القرار باسم الشخص المعنوي، أو سلطة ممارسة الضبط داخل الشخص المعنوي.
- بالإضافة إلى الحالات التي سبق النص عليها في الفقرة الأولى فإنه يجب على كل طرف أن يتخذ الإجراءات الضرورية من أجل التأكد من أن الشخص المعنوي يمكن أن يكون مسؤولاً إذا تخلفت المراقبة والضبط من قبل شخص طبيعي مشار إليه في الفقرة1 قد جعل من الممكن ارتكاب الجرائم المشار إليها في الفقرة السابقة لحساب الشخص المعنوي عن طريق شخص طبيعي يتصرف تحت سلطته.
- تكون نطاق مسؤولية الشخصية المعنوية في نطاق المسؤولية الإدارية والجنائية والمدنية، حسب الجريمة المقترفة.
- كما أن مسؤولية الشخص المعنوي لا تعفي الشخص الطبيعي من المسؤولية.

وقد ورد النص بالفرنسي:

Article 12 – Responsabilité des personnes morales

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:
a- sur un pouvoir de représentation de la personne morale;
b- sur une autorité pour prendre des décisions au nom de la personne morale;
c- sur une autorité pour exercer un contrôle au sein de la personne morale.
2- Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.
3- Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.
4- Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

راجع هلالي عبد اللاه، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص149.وراجع: الموقع الإلكتروني لمكافحة الجريمة الاقتصادية، مرجع سابق، على الرابط:

- http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

ومن خلال نص المادة سالفة الذكر يتضح بأن المشرع الجزائري قد شدد عقوبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذا ارتكبت من قبل الشخص المعنوي، لأن الشخصية المعنوية عندما تعاقب بعقوبة الشخص الطبيعي- عقوبة الغرامة - فإن العقوبة قد لا تكون مجدية، ولا تشكل عبئا كبيرا عليها ، ولذلك فإن مضاعفتها إلى خمس مراتمقارنةً بالعقوبة المحكوم بها على الشخص الطبيعي، قد يكون ذلك سببا في الحد من ارتكاب تلك الجرائم من قبل الأشخاص المعنوية، ومع ذلك فهي بحاجة إلى إعادة نظر، حيث تم تشديدها لدرجة أنها قد تتسبب في إفلاس الشخصية المعنوية.

2- الركن المادي

يتكون الركن المادي للجريمة المعلوماتية المنصوص عليها في القسم السابع من ق.ع.ج من الأفعال المادية الخاصة بكل جريمة على حدة، والتي سيتم إيضاحها أثناء تناول الجرائم المعلوماتية كلا على حدة، وعلى سبيل المثال في جريمة الدخول أو البقاء فإن الركن المادي يتمثل بفعل الدخول وفعل البقاء، وهكذا بالنسبة لباقي الجرائم، وما يميز الركن المادي في الجرائم المعلوماتية المرتكبة من قبل الشخص المعنوي هو:

أ- أن الأفعال المادية للجريمة ترتكب عن طريق شخص يمارس سلطة القيادة داخل الشخص المعنوي.

ب- أن الجريمة ترتكب باسم الشخص المعنوي ولحسابه .

ج- يجب أن يكون الشخص الذي ارتكب الجريمة يمارس سلطة اتخاذ القرار.

د- أن يقوم الشخص المعنوي باقتراف أي من الأفعال المشار إليها سلفا، وهي فعل الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، أو تغيير أو محو أو تعديل معطيات الحاسوب، أو التعامل في معطيات غير شرعية ناتجة أو يمكن أن ترتكب بها إحدى جرائم المعلوماتية، ومن تلك الأفعال التصميم،البحث، التجميع ،التوفير، النشر،الاتجار[1].

([1]) توضح المادة (12) من اتفاقية بودابست السالف الإشارة إليها مسؤولية الشخصية الاعتبارية أو المعنوية بالنسبة للأفعال الجنائية المرتكبة لحسابها، عن طريق شخص يمارس سلطة القيادة داخل الشخص المعنوي، كما تقرر مسؤولية الشخص الذي يمارس سلطة القيادة إذا ترك مراقبة أو ضبط مستخدم أو عميل الشخص المعنوي إذا كان من شأن الترك أو التسهيل أن يتسبب في ارتكاب إحدى جرائم المعلوماتية المنصوص عليها في الاتفاقية، وأن تكون الجريمة قد ارتكبت لصالح الشخص المعنوي، أو أن يكون الشخص الطبيعي الذي ارتكب الجريمة يتبوأ مكانة عالية، أو يمارس سلطة القيادة في المؤسسة -المدير مثلا-، أو أن يملك سلطة اتخاذ القرار، كما تقر ذات المادة=

3- الركن المعنوي

يتحقق الركن المعنوي في الجرائم المعلوماتية المرتكبة من الشخص المعنوي إذا توافر القصد الجنائي العام بعنصرية العلم والإرادة.

فيشترط لقيام الجريمة المعلوماتية المرتكبة من الشخص المعنوي، أن يكون من ارتكب الجريمة باسم الشخص المعنوي، أو لحسابه، عالما بأنه يرتكب جريمة من الجرائم التي تضمنها القسم السابع مكرر من ق.ع.ج.

كما يجب أن تتوافر الإرادة لاقتراف إحدى جرائم المعلوماتية من قبل ممثل الشخص المعنوي، أو من يمارس سلطة اتخاذ القرار باسمه.

4- العقوبات

تطبق على الشخص المعنوي نوعان من العقوبات، منها عقوبات وردت في نصوص قانون العقوبات بشكل عام، ومنها عقوبات وردت - في قانون العقوبات- بنصوص خصت الجرائم المعلوماتية المرتكبة من الشخص المعنوي.

أ- عقوبات الجرائم المرتكبة من الشخص المعنوي بشكل عام

تضمن قانون العقوبات الجزائري على عدد من العقوبات في حال ارتكاب الشخص المعنوي لجناية أو جنحة منصوص عليها في القانون، منها عقوبة الغرامة كعقوبة أصلية إضافة إلى عدد من العقوبات التكميلية.

1) **العقوبة الأصلية:** وتتمثل في الغرامة التي تساوي من مرة إلى خمس مرات للعقوبة المقررة على الشخص الطبيعي[1].

=المسؤولية على من يرتكب الجريمة تحت رقابة وإشراف الشخص المعنوي- مستخدماً كان أو عميلاً - بشروط هي: أن يتم ارتكاب الجريمة من عميل أو مستخدم للشخص المعنوي، وأن تكون الجريمة التي ارتكبت لصالح الشخص المعنوي، وأن يكون ارتكاب الجريمة نتيجة لتقاعس من بيده سلطة القيادة والإشراف والرقابة على المستخدم أو العميل، دون استلزام فرض رقابة على اتصالات المستخدمين، وبناء على ذلك فإن مقدم الخدمات لا يمكن أن مسؤولاً عن جريمة ترتكب عبر جهازه عن طريق مستخدم أو زبون أو شخص ثالث، لأن مصطلح شخص طبيعي Natural Person يعمل تحت سلطته لا ينطبق إلا على المستخدمين والعملاء الذين يتصرفون في إطار سلطاتهم. راجع هلالي عبد اللاه، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص150.

([1]) راجع: الفقرة (1) من المادة (18 مكرر) من القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004 المُعَّدِلْ والمُتَمِّمْ لقانون العقوبات الجزائري، وقد أبقاها المشرع الجزائري كما هي في التعديل الأخير بالقانون رقم (06 – 23) المؤرخ في 20 ديسمبر 2006.

2) العقوبة التكميلية: يعاقب الشخص المعنوي بواحدة أو أكثر من العقوبات التكميلية التالية[1]:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
- المنع من ممارسة نشاط أو عدة أنشطة مهنية.
- نشر الحكم وتعليقه.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

والعقوبات السابقة ليست خاصة بالجرائم المعلوماتية، وإنما يمكن أن توقع على كل الجرائم التي يرتكبها الشخص المعنوي، كما أن عقوبة الغرامة ذات حدين أدنى وأعلى، وبالتالي فإن للقاضي الحق في تفريد العقوبة.

ب- عقوبات الشخص المعنوي في جرائم المعلوماتية

العقوبة التي نصت عليها المادة(394مكرر4) للشخص المعنوي الذي يرتكب إحدى جرائم المعلوماتية هي عقوبة الغرامة، والتي حددها المشرع الجزائري بحد واحد، فلم يترك للقاضي الحق في تفريد العقوبة بين حد أدنى وحد أقصى كما في المادة(18 مكرر ع.ج) ، بل إن القاضي مقيد بتطبيق حد واحد للغرامة، وهي تساوي خمس مرات للعقوبة المقررة للشخص الطبيعي، وبذلك فتكون عقوبات الجرائم المعلوماتية وفقا للقانون الجزائري كما يأتي :

1) عقوبة جريمة الدخول أو البقاء في صورتها العادية

تكون عقوبة جريمة الدخول والبقاء المرتكبة من قبل الشخص المعنوي هي الغرامة خمسة أضعاف عقوبة الجريمة المرتكبة من الشخص الطبيعي، فتكون من(50.000×5=250.000دج"مائتين وخمسين ألف دينار" إلى100.000×5=500.000دج"خمسمائة ألف دينار"[2].

([1]) الفقرة (2) من المادة (18 مكرر) من القانون. رقم (06 – 23) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات، وهي نفس المادة في القانون السابق له (نوفمبر 2004) عدى إضافة كلمة التكميلية في القانون الجديد بحيث أصبحت العبارة " واحدة أو أكثر من العقوبات التكميلية".

(2) راجع: المادتين (394 مكرر، و394 مكرر4) من القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004.

2) عقوبة جريمة الدخول أو البقاء في صورتها المشددة[1]

تختلف عقوبة جريمة الدخول والبقاء المرتكبة من قبل الشخص المعنوي بحسب النتيجة المترتبة على الدخول والبقاء:

أ) إذا نتج عن الدخول أو البقاء حذف أو تغيير لمعطيات النظام

تكون العقوبة من(50.000×2×5=500.000دج خمسمائة ألف إلى 100.000×2×5=1.000.000دج مليون دينار)

ب) إذا نتج عن الدخول أو البقاء تخريب نظام اشتغال النظام

وفي هذه الحالة تكون العقوبة من(50.000 ×5=250.000دج مائتان وخمسين ألف دينار إلى(150.000×5=.750.000سبعمائة وخمسين ألف دينار.

3) عقوبة جريمة التلاعب بالمعطيات

تكون عقوبة جريمة التلاعب بالمعطيات سواءً بإدخال معطيات عن طريق الغش إلى نظام المعالجة الآلية للمعطيات، أم بالحذف، أم التعديل للمعطيات التي يتضمنها النظام من(500.000×5=2.500.000دج مليونين ونصف إلى(2.000.000×5=10.000.000دج عشرة ملايين دينار)[2].

4) عقوبة التعامل في معطيات غير شرعية

في هذه الحالة تكون العقوبة من(1.000.000×5=5.000.000دج خمسة ملايين دج إلى 5.000.000×5=25.000.000دج خمسة وعشرين مليوناً)[3].

---

(1)راجع: المادتين (394 مكرر، و394 مكرر4) من القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004 المُعَدِلْ والمُتَمِمْ لقانون العقوبات الجزائري..

(2) راجع المادتين (394 مكرر1، و394 مكرر4) من القانون السابق.

(3) راجع المادتين 394 مكرر 2، و394 مكرر4 من القانون نفسه.

المطلب الخامس

العقوبات التكميلية للجرائم المعلوماتية

بالإضافة إلى الأحكام المشتركة للجريمة المعلوماتية السالف ذكرها، فإن الجرائم المعلوماتية تشترك في العقوبات التكميلية –المتعلقة بالجنح - المنصوص عليها في قانون العقوبات الجزائري بشكل عام [1]، بالإضافة إلى عقوبتي المصادرة والإغلاق اللتين تضمنتهما المادة (394 مكرر6) كعقوبتين تكميليتين تخص الجرائم المعلوماتية[2]، وقد نصت عليها عدد من القوانين العربية الخاصة بمكافحة جرائم المعلوماتية[3].

1. العقوبات التكميلية للجرائم المرتكبة من الشخص الطبيعي بشكل عام

العقوبات التكميلية التي وردت في ق.ع.ج يمكن تطبيقها على الجرائم المعلوماتية بالنسبة للعقوبات التي نص القانون بتطبيقها على الجنح، أو على الجنايات والجنح، وجميع تلك العقوبات جوازية وليست وجوبية كما في بعض عقوبات الجنايات وهي:

- الحجز القانوني، وهي عقوبة وجوبيه بالنسبة للجنايات ومن ثم فهي جوازيه بالنسبة للجنح ومنها الجرائم المعلوماتية.
- تحديد الإقامة، وتتمثل بإلزام المحكوم عليه أن يقيم في نطاق إقليمي يحدده الحكم لمدة لا تتجاوز خمس سنوات [4].

---

(1)انظر المواد من(9 إلى 18) من القانون الجزائري رقم (06 – 23) المؤرخ في 20 ديسمبر سنة 2006) المُعَّدِلْ والمُتّ ًمِمْ للأمر رقم (66 – 165) المؤرخ في 8يونيو سنة 1966المتضمن قانون العقوبات. وقد سار التشريع الجزائري على ضوء التشريع الفرنسي في إقرار تلك العقوبات، حيث نص ق.ع.ف على العقوبات التكميلية في تشريعاته المتعاقبة، 1988، و1994،2004 ، إذ لم تكن المادة(462) فقره (9) من قانون 88 تقرر سوى عقوبة تكميلية واحدة وهي المصادرة، أما المادة (323-5)من ق.ع.ف لسنة 1994، والمادة نفسها من ق.ع لسنة 2004 فقد تضمنت قائمة من العقوبات التكميلية لتعطي القاضي إمكانية تفريد العقوبة وهي ذات العقوبات التي نص عليها التشريع الجزائري مؤخرا.لمزيد من التفصيل راجع:محمد خليفه،مرجع سابق، ص122.

(2) راجع: المادة (394 مكرر6) من القانون رقم(04 – 15) المؤرخ في 10 نوفمبر 2004 المُعّدِلْ والمُتّ ًمِمْ لقانون العقوبات الجزائري.

(3) ومن القوانين العربية التي نصت على العقوبات التكميلية للجرائم المعلوماتية نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم(م/17) المؤرخ في 1428/3/8هـ بناء على قرار مجلس الوزراء رقم (79)المؤرخ في 1428/3/7هـ حيث نصت المادة (13) منه على:(مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقا نهائيا أو مؤقتا متى كان مصدرا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه)، وكذلك القانون الإماراتي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات حيث نصت المادة (24) منه :(مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو الموقعالذي يرتكب فيه أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكه، وذلك إغلاقاً كلياً أو للمدة التي تقدرها المحكمة).

(4) راجع: المادة(11) من ق.ع.ج.

- المنع من الإقامة لمدة لا تزيد عن خمس سنوات بالنسبة للجنايات(1).
- الحرمان من ممارسة الحقوق الوطنية، والمدنية، والعائلية لمدة لا تزيد عن خمس سنوات(2).
- المصادرة الجزئية للأموال.
- المنع المؤقت لمدة لا تتجاوز خمس سنوات من ممارسة مهنة أو نشاط إذا ثبت علاقة المهنة أو النشاط بالجريمة المرتكبة،وأن ثمة خطراً في استمرار ممارسة المهنة أو النشاط(3).
- إغلاق المؤسسة لمدة لا تزيد عن خمس سنوات بالنسبة للجنح(4).
- الإقصاء من الصفقات العمومية لمدة لا تزيد عن خمس سنوات في الجنح، ومنها جرائم المعلوماتية(5).
- الحظر من إصدار الشيكات أو بطاقات الدفع، وتكون بالنسبة للجنح خمس سنوات(6).

(1) تضمنت المادة (12) من ق.ع.ج رقم (06- 23) المؤرخ في 20 ديسمبر 2006 تعريف المنع من الإقامة بأنه: حظر تواجد المحكوم عليه في بعض الأماكن لمدة لا تزيد عن خمس سنوات في مواد الجنح، وعشر سنوات في الجنايات، بخلاف قرار المنع من الإقامة بالتراب الوطني، التي تكون مدتها 10 سنوات أو نهائية، وتطبق على كل أجنبي ارتكب جناية أو جنحة.راجع الجريدة الرسمية رقم 84،ص 13.

(2) خولت المادة(14) من ق.ع.ج 2006 للمحكمة عند قضائها في جنحة بجواز حظر ممارسة حق أو أكثر من الحقوق الوطنية، والمدنية، والعائلية المنصوص عليها في المادة (9 مكرر) وهذه الحقوق وفقا للمادة الأخيرة هي :
- العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة
- الحرمان من حق الانتخاب والترشيح ومن حمل أي وسام.
- عدم الأهلية لأن يكون مساعدا محلفا، أو خبيرا، أو شاهدا على أي عقد، أو شاهدا أمام القضاء إلا على سبيل الاستدلال.
- الحرمان من الحق في حمل الأسلحة، وفي التدريس، أو في إدارة مدرسة، أو الخدمة في مؤسسة للتعليم بوصفه أستاذا، أو مدرسا، أو مراقبا.
- عدم الأهلية لأن يكون وصيا أو مقدما.
- سقوط حق الولاية كلها أو بعضها. وتطبق تلك العقوبات من تاريخ انقضاء العقوبة السالبة للحرية أو الإفراج عن المحكوم عليه.

(3) المادة (16) من القانون رقم (06- 23) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري.

(4) وهي عقوبة تطبق بالنسبة للجنايات والجنح إلا أنها في الجنايات عشر سنوات وفي الجنح خمس سنوات .راجع المادة (16 مكرر 1) من ق .ع.ج.

(5) والإقصاء من الصفقات العمومية تعني منع المحكوم عليه من المشاركة بصفه مباشره أو غير مباشرة في أي صفقة عمومية وقد تكون بصوره نهائية أو لمدة عشر سنوات بالنسبة للجنايات، وخمس سنوات بالنسبة للجنح، ونحن إذ نشير إلى العقوبة المتعلقة بالجنح في المتن، لأنها هي التي يمكن تطبيقها على الجرائم المعلوماتية .راجع المادة (16 مكرر 2) ع.ج.

(6) وبالنسبة للجنايات فتكون مدة الحظر من إصدار الشيكات أو استعمال البطاقات هي عشر سنوات. راجع: المادة (16 مكرر3) من ق.ع.ج.

- تعليق أو سحب رخصة السياقة، أو إلغائها مع المنع من استصدار رخصة جديدة، ويكون الحظر لمدة خمس سنوات[1].
- سحب جواز السفر، ولمدة خمس سنوات [2].
- نشر الحكم أو تعليق حكم أو قرار الإدانة [3].

وكما أن ق.ع.ج قد نص على العقوبات التكميلية ضمن النصوص التقليدية للجنايات والجنح، كما نص على عقوبتي المصادرة والإغلاق ضمن النصوص المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، وجعل بعضها وجوبية – في بعض الجنايات- وبعضها جوازيه – في الجنايات والجنح- ، فإن ق.ج.ع.ي قد نص على العقوبات التكميلية في نصوصه التقليدية للجرائم بشكل عام، سواء أكانت جسيمة أم غير جسيمة، وجعلها جوازيه وليست وجوبيه [4] باستثناء مصادرة الأشياء المضبوطة التي يعد صنعها، أو

([1]) وتطبق على الجنايات والجنح، وتكون مدة الحظر متساوية وهي خمس سنوات.راجع: المادة (16 مكرر 4) من القانون رقم (06- 23) المؤرخ في 20 ديسمبر 2006(ج.ر رقم 84،ص 13).

([2]) المادة 16 مكرر 5 من نفس القانون.

([3]) المادة 18 من نفس القانون.

([4]) تضمنت المواد من (100 :103) من ق.ج.ع.ي لسنة 1994 العقوبات التكميلية التي يمكن تطبيقها في حالة ارتكاب جريمة من الجرائم، وتركت للقاضي سلطة تقديرية في الحكم بتلك العقوبات والاستعانة بعدد من الأمور التي تدل على أن الجاني يستحق تطبيق عقوبة أو أكثر من العقوبات التكميلية ومنها طبيعة الجريمة، والسوابق الجنائية، وتتوقف على نطق القاضي بها، ولا يجوز تنفيذها على المحكوم عليه إذا لم ينص عليها الحكم وتتمثل في: الحرمان من كل أو بعض الحقوق، والوضع تحت المراقبة لمدة لا تقل عن سنة ولا تزيد عن ثلاث سنوات، تبدأ من يوم انقضاء عقوبة الحبس، والمصادرة للأشياء المضبوطة التي تحصلت من الجريمة أو التي استعملت في ارتكابها أو التي كانت معدة لاستعمالها فيها. والحقوق التي يحرم مرتكب الجريمة من أحداها أو بعضها هي:

- الحرمان من تولي الوظائف والخدمات العامة، أو الوظائف والخدمات النيابية والمهنية
- الحرمان من تولي إدارة مدرسة أو ممارسة أي نشاط تعليمي.
- من أن يكون ناخبا أو منتخبا في المجالس العامة.
- عضوا في مجلس إدارة شركة أو مديرا لها.
- صاحب التزام أو امتياز من الدولة.
- وصيا أو قيما أو وكيلا.
- خبيرا أو شاهدا في عقد أو تصرف.
- مديرا أو ناشرا أو محررا لإحدى الصحف.
- من حمل أوسمة وطنية أو أجنبية.
- من حمل أي سلاح.
- الحرمان من استمرار مزاولة المهنة
- تحديد مكان الإقامة
- إغلاق المحل .
- حرمان الأجنبي من الاستمرار في الإقامة في البلاد.

وإذا كان المحكوم عليه وقت صدور الحكم متمتعا ببعض هذه الحقوق وحرم منها نفذ الحرمان بمجرد صدور الحكم، ويكون الحرمان بصفة دائمة فلا يزول أثره إلا برد الاعتبار، كما يجوز أن يكون مؤقتا بمدة لا تقل عن سنة، ولا تزيد عن ثلاث سنوات تبدأ من تاريخ انتهاء تنفيذ العقوبة الأصلية أو من تاريخ انقضائها

حيازتها، أو إحرازها، أو استعمالها، أو بيعها، أو عرضها للبيع جريمة في ذاتها، ولو لم تكن مملوكة للمتهم أو لم يحكم بإدانته، مع مراعاة حقوق الغير حسن النية.

ونظرا لكون التشريع اليمني لم يتضمن نصوصاً عقابية مستحدثه تعاقب على اقتراف الجرائم المعلوماتية مثل التشريع الجزائري، ولكون العقوبات التكميلية إنما أقرت كعقوبات تكميلية للعقوبات الأصلية، فإن العقوبة التكميلية لا يمكن تطبيقها مستقلة عن العقوبة الأصلية.

وبالتالي فإن الجرائم المعلوماتية التي يمكن أن تنطبق عليها العقوبات الأصلية في ق.ج.ع.ي، وتتيح للقاضي كذلك حق تطبيق عقوبة أو أكثر من العقوبات التكميلية المنصوص عليها، باستثناء عقوبة المصادرة الوجوبية، لكون القانون اليمني لم ينص عليها، أما الجرائم التي لا يمكن تطبيق النصوص التقليدية عليها، وتحتاج إلى نصوص تتناسب مع حداثتها فلا يمكن تطبيق عقوبة تكميلية عليها من باب أولى ، طالما أنه لا يمكن تطبيق العقوبة الأصلية، وبيان ذلك يكون من خلال موقف القانون اليمني بصدد كل جريمة على حدة، وفقاً لما سيتم إيضاحه أثناء تناول الأحكام الخاصة بكل جريمة.

2. العقوبات التكميلية المتعلقة بجرائم المعلوماتية

تضمن نص المادة(394 مكرر6) على العقوبات التكميلية التي يجب على القاضي تطبيقها في حالة ارتكاب إحدى جرائم المعلوماتية، حيث ورد النص: (مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها)[1]. ومن خلال النص يتضح بأن المشرع الجزائري قد ضمن عقوبتين تكميليتين

---

[1] والنص بالفرنسي :

Art. 39 4 octiès.- (Loi n 04 – 15 du10 novembre 2004)
Sans préjudice des droits des tiers de bonne foi, il sera procédé à la confiscation des instruments, programmes et moyens utilisés dans la commission de l'infraction ainsi qu'à la fermeture des sites, objets de l'une des infractions prévues à la présente section' et des locaux et lieux d'exploitation dans le cas où le propriétaire en est informé.

تطبق في حال ارتكاب إحدى جرائم المعلوماتية وهي المصادرة والغلق، وفيما يلي توضيح لكلا العقوبتين.

أ- عقوبة المصادرة

يقصد بعقوبة المصادرة: الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة أو ما يعادل قيمتها عند الاقتضاء[1].

ويبدو أن المصادرة وفقا لنص المادة(394 مكرر6) من ق.ع .ج سالفة الذكر هي عقوبة وجوبية، لأنها لم تترك الخيار للقاضي بين الحكم، وعدم الحكم بها كما في العقوبات الأصلية والمشددة للجريمة، وكذلك لأن الهدف من هذه العقوبة هو الحد من تلك الجرائم ، فأصحاب الأجهزة والوسائل عندما يعلمون مسبقا بأنه سوف تتم المصادرة لكل الأجهزة والوسائل التي ترتكب بها الجريمة، بالإضافة إلى العقوبات الأصلية التي ستوقع عليهم، فإن ذلك سيكون مانعا من الإقدام على ارتكاب تلك الجرائم ، ولتطبيق عقوبة المصادرة فإنه يتطلب توافر بعض الشروط منها:

- يجب أن تكون عقوبة المصادرة تالية لعقوبة أصلية من العقوبات المنصوص عليها في القانون، وهي الحبس أو الغرامة، وتكون العقوبة وجوبية في الجنايات والجنح وليست جوازية، إلا أنها تكون وجوبية في الجنايات بشكل عام، أما في الجنح والمخالفات فلا تكون وجوبيه، إلا إذا نص القانون على تلك العقوبات[2]، وذلك ما ينطبق على عقوبة المصادرة في جرائم المساس بأنظمة المعالجة الآلية للمطيات، حيث تطلب الأمر النص على عقوبة المصادرة لأن تلك الجرائم داخلة في الجنح[3].
- أن تتم مصادرة الأجهزة والوسائل التي استخدمت في ارتكاب الجريمة مهما كانت تلك الوسائل تقليدية أو معلوماتية، فقد يستخدم كتاب لتوضيح وشرح كيفية ارتكاب الجريمة المعلوماتية، وقد يستخدم برنامج، ولا يشترط أن تكون الوسائل والأجهزة التي يتم مصادرتها كعقوبة تكميلية محددة على سبيل الحصر، وإنما تنطبق العقوبة على أية وسيلة كانت، ويجب أن تكون الأشياء التي يحكم بمصادرتها قد تم ضبطها من قبل الجهات المختصة.

([1]) راجع: المادة (15) من ق.ع.ج رقم (06 – 23) المؤرخ في 20 ديسمبر سنة 2006المُعَدِّلِ وَالمُتَمِّمْ للأمر رقم (66 – 165) المؤرخ في 8 يونيو سنة 1966والمتضمن قانون العقوبات.

([2]) راجع المادة (15 مكرر 1) من نفس القانون(ج ر84 ص.13).

([3]) راجع المادة (394 مكرر4) من القانون رقم(04- 15) المؤرخ في 10نوفمبر 2004.

- يجب أن لا تمتد عقوبة المصادرة على حقوق الغير حسن النية [1]، وهذا القيد نابع من طبيعة العقوبة كونها عقوبة شخصية يجب أن لا تطال الغير حسن النية، والغير هو: كل أجنبي عن الجريمة تماما، ومبررات عدم عقوبة حسن النية لأنه لم يكن يعلم بأن تلك الأجهزة سوف تستخدم في ارتكاب الجريمة، فلم يتوافر بحقه القصد الجنائي العمدي أو حتى الخطأ. ولا تقتصر حقوق الغير حسن النية على حق الملكية فحسب، بل إن الحقوق الأخرى مثل حق الانتفاع والرهن يسري عليها ما يسري على حقوق الملكية، ولا تشملها عقوبة المصادرة بحق حسن النية. [2].

ب- عقوبة الغلق

نصت المادة (394 مكرر6) على عقوبة الغلق إلى جانب عقوبة المصادرة كعقوبتين تكميليتين، يعاقب بهما كل من ارتكب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في القانون.

وتشمل غلق المواقع التي استغلت، أو استخدمت في ارتكاب أي من جرائم المعلوماتية المنصوص عليها في القسم السابع مكرر ع.ج، وكذلك غلق المحلات، أو أماكن الاستغلال التي ارتكبت منها تلك الجرائم إذا ارتكبت بعلم مالكها.

ويرى البعض بأن المشرع الجزائري لم يكن موفقا في استعمال عبارة "إغلاق المواقع التي كانت محلا للجريمة" لكون هذا اللفظ يمكن استخدامه للمواقع التي تم الاعتداء عليها أو التلاعب بمعطياتها، ومن غير المعقول غلقها كونها ضحية، وكان الأولى أن تكون عبارة النص "المواقع التي تستعمل في ارتكاب الجريمة "بدلا من المواقع التي تعد محلا للجريمة[3].

وهذا الرأي قد جانبه الصواب، ذلك بأن المشرع إنما يقصد بالمواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها، أي التي ترتكب من خلالها تلك الجرائم، فقد تكون محلا لارتكاب تلك الجرائم عندما يتم من خلالها إرسال برامج للتدمير أو التجسس، أو لأي غرض غير مشروع، ويتسبب في الاعتداء على أنظمة ومواقع الغير،

---

(1) يعتبر من الغير حسن النية الأشخاص الذين لم يكونوا محل متابعة أو إدانة من أجل الوقائع التي أدت إلى المصادرة، ولديهم سند ملكية أو حيازة صحيح ومشروع على الأشياء القابلة للمصادرة.راجع: المادة (15مكرر2) من ق.ع.ج رقم(06 – 23) المؤرخ في 20 ديسمبر سنة 2006.

(2) محمد خليفة، مرجع سابق، ص121.

(3)محمد خليفة، مرجع سابق، ص123.

كما قد تكون محلا للجريمة عندما تكون عبارة عن محتوى للأعمال الضارة والإباحية، وذلك عندما تشمل على معلومات وبيانات لتعليم الجريمة يستطيع من خلالها من يدخل على تلك المواقع من المجرمين، أو من لهم ميول إجرامية أن يجد ضالته في تلك المواقع، بل إن تأثيرها لا يقتصر على أولئك فحسب، وإنما قد يقع فيها العديد من الأبرياء التي تؤثر عليهم تلك المواقع وقد تجرهم إلى الانحلال وكافة أشكال الإجرام المعلوماتي.

كما أن ما يؤكد صحة تفسير العبارة " مع إغلاق المواقع التي تكون محلا لجريمة" بأنها المواقع التي ترتكب منها جرائم المعلوماتية، أو تكون محتوى للأعمال الضارة أو الإباحية، النص المكمل لها بحيث تكون العبارة بكاملها " مع إغلاق المواقع التي تكون محلا لجريمة، من الجرائم المعاقب عليها وفقا لهذا القسم" فهذه العبارة في مقطعها الثاني تؤكد بأن المواقع التي نص المشرع على إغلاقها هي التي ارتكبت من خلالها أو بواسطتها تلك الجرائم، حيث إن النصوص القانونية الخاصة بكل جريمة من تلك الجرائم المنصوص عليها، سواء تعلقت بالدخول أم البقاء ،أم التلاعب في المعطيات وغيرها من الجرائم، تعاقب من يقوم بالدخول أو البقاء أو التلاعب، وكل تلك الألفاظ، تشير إلى أن الاعتداء أو الفعل الإجرامي المرتكب قد يتم من موقع أو نظام، وهو الموقع محل الجريمة ويستهدف موقعاً أو نظاماً آخر، وهو الموقع أو النظام الضحية.

أخيرا فإن عقوبة الغلق تشمل غلق المواقع التي تكون محلا لجريمة من الجرائم المعلوماتية، كما تشمل أيضا إغلاق المحل أو مكان الاستغلال بشرط أن تكون الجريمة قد ارتكبت بعلم مالكها، وعليه إذا انتفى علم مالك المحل أو مكان الاستغلال فلا تطبق العقوبة، وعقوبة الغلق مثلها مثل عقوبة المصادرة لا تقع في مواجهة الغير حسن النية للأسباب السالف ذكرها.

المبحث الثاني

الأحكام الخاصة بالجرائم المعلوماتية المستحدثة

بعد أن تم إيضاح الأحكام المشتركة للجرائم المعلوماتية - بهدف تجنب التكرار- أثناء شرح أركان كل جريمة، يتبقى لنا تناول الأحكام الخاصة بكل جريمة، لما لهذه الجرائم من أهمية، كونها مستحدثة تزامن ظهورها وتطورها مع ظهور وتطور تكنولوجيا الإعلام والاتصال والمعلوماتية، ومع ذلك فما زالت تفتقر إلى الشرح والإيضاح الكافي لأركانها، كما أن أحكام القضاء مازالت قلية بشأنها وعلى وجه الخصوص في الدول العربية، لأسباب منها محدودية الجرائم المرتكبة، وقلة القوانين التي صدرت لمواجهتها، بخلاف الدول المتقدمة.

وقد تضمن قانون العقوبات الجزائري النص على الجرائم المعلوماتية المستحدثة في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد(394مكرر : 394 مكرر 7) [(1)].

وبالمقابل فلم يتضمن قانون العقوبات اليمني مثل تلك النصوص، وإن كان مشروع قانون حق الحصول على المعلومة قد أشار بصورة مقتضبة إلى بعضها إثناء التطرق إلى حماية المعلومات، إلا أنه بالإضافة إلى القصور الذي يعتريه، فهو كذلك لم يرى النور حيث مازال مشروعا حتى الانتهاء من إعداد هذه الدراسة، لذلك فلا يكون أمام الباحث سوى بيان موقف قانون العقوبات من تلك الجرائم كلما استوجب الأمر ذلك، بخلاف القانون الجزائري الذي سيتم توضيح تلك الجرائم على ضوء نصوصه، وسيتم التنويه إلى نصوص القانون الفرنسي ذات العلاقة بالدراسة، وبعض القوانين الأخرى، كما سيتم إيضاح بعض الجرائم التي أغفلها المشرع الجزائري على ضوء القانون الفرنسي مثل جريمة الاعتداءات العمدية على نظم المعالجة الآلية للمعطيات.

([1]) راجع : القسم السابع من قانون العقوبات الجزائري رقم (04- 15) المؤرخ في 10 نوفمبر 2004المَعدِل والمتمِم للأمر رقم(66- 156) المؤرخ في 8 يونيو 1966، ط4، الديوان الوطني للأشغال التربوية، 2005، ص124، ص125، وراجع: يوسف دلاندة، مرجع سابق، ص259، وص260، وص261.

المطلب الأول

جريمة الدخول والبقاء في نظام المعالجة الآلية

الولوج غير القانوني(Illegal access)

تعتبر السويد أول دولة قامت بسن قانون يتعلق بجرائم الكمبيوتر والإنترنت، تضمن عقوبة جريمة الدخول والبقاء في نظام الكمبيوتر المملوك للغير[1]، وقد تباينت التشريعات في تجريم الدخول أو البقاء، فبعضها تجرم الدخول في نظام معلوماتي بشكل مطلق دون أن تستلزم توافر القصد الخاص، ولا تستلزم كذلك قيداً معيناً يتعلق بالركن المادي، ومن تلك التشريعات التشريع الفرنسي والتشريع الجزائري، ومنها ما يقيد تجريم الولوج غير الشرعي (Illegal access) إلى نظام المعالجة الآلية للمعطيات بتوافر عنصر بالركن المادي، وذلك باستلزام أن يكون الدخول إلى أنظمة معينة كالأجهزة الحكومية، وأجهزة المؤسسات المالية، والأجهزة التي تحوي معلومات تتعلق بالأمن القومي أو العلاقات مع الدول الأجنبية .

1- الركن الشرعي لجريمة الدخول والبقاء

جرم المشرع الجزائري جريمة الدخول والبقاء إلى نظام المعالجة الآلية للمعطيات باعتبارها من الجرائم المستحدثة التي تزامن ظهورها مع التطور التكنولوجي لعلم الاتصالات والمعلومات، وبالتالي فقد وضع حدا لأي خلاف فقهي أو قانوني حول تجريمها، عملا بالمبدأ المعروف بالشرعية الذي مفاده بأن لا جريمة ولا عقوبة إلا بنص قانوني.

---

(1) تعد دولة السويد هي الدولة الأولى التي سنت قانوناً يعاقب على جريمة الدخول في نظام المعالجة الآلية للمعطيات، حيث أصدرت قانون البيانات السويدي لعام 1973، الذي عالج قضايا النصب عن طريق الحاسب الآلي، إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها . وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي (1976م – 1985). راجع شيماء عبد الغني محمد عطا الله: الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، 2005 ، ص110 ، وراجع حسن عزيز نور الحلو:الإرهاب في القانون الدولي، رسالة ماجستير،الأكاديمية العربية المفتوحة ،الدانمرك، 2007، ص151.
راجع : موقع كلية الحقوق جامعة المنصورة، ت.د 2008/5/20
http://www.f-law.net/law/showthread.php?t=6420
كما نشرت الرسالة في شبكة المعلومات الدولية بصيغة ملف ورد على الرابط،
http://www.scribd.com/doc/26849840/%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8-%D9%81%D9%8A-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A

بخلاف المشرع اليمني حيث لم يتضمن في نصوصه ما يدل من قريب أو بعيد على تجريمها.

حيث نصت المادة (394 مكرر)ع.ج على أن (يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000دج)[1].

من خلال النص القانوني للمادة سالفة الذكر يتضح بأن المشرع الجزائري قد حذا حذو التشريع الفرنسي في تجريم جريمة الدخول والبقاء في نظام المعالجة الآلية للمعطيات، حيث استمد النص منه [2].

([1]) المادة (394 مكرر) من قانون العقوبات الجزائري رقم (04 – 15)المؤرخ في 10 نوفمبر 2004المُعَّدِلْ و المُتَّمِم للأمر رقم (66 -156) المؤرخ في 18صفرعام 1386الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات.ونص المادة بالفرنسي:

Art 394 bis. -(Loi n° 04 – 15 du 10 novembre 2004) Est puni d'une peine d'emprisonnement de trios (3) mois à un (1) an et d'une amende de 50.000 DA à 100.000 DA, quiconque accède ou se maintient, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ou tente de le faire

La peine est portée au double lorsqu"il en est résulte soit le suppression soit le modification de données continues dans le système.

Lorsqu"il en est résulté une altération du fonctionnement de ce système la peine est de six (6) mois a deux (2) ans d' emprisonnement et d'une amende de 50. 000 da a 150 .000 DA)

([2]) حيث يقابل نص المادة(394) ع.ج نص المادة (323/ 1) من القانون الفرنسي الصادر في أول مارس عام 1994 ونفس المادة بالقانون المعدل 2004، واللتان تضمنتا النص على تجريم الدخول بطريق الغش في اتصال مع نظام لمعالجة المعلومات آليا سواء كان الدخول إلى النظام كله أم إلى جز منه، وقررت لذلك عقوبة الحبس سنه (1) والغرامة 100.000 فرنك إلى الحبس سنتين (2) والغرامة 200.000 فرنك فرنسي إذا ترتب على الدخول والبقاء محو أو تعديل في المعطيات المخزنة في النظام أو إتلاف تشغيل النظام، وذلك وفق نص المادة 1/323 من ق.ع 94، أما ق.ع.2004 فقد شدد العقوبة بدلا من عام إلى عامين في حالة الدخول والغرامة 30000 ألف اورو، كما ضاعفت العقوبة في حالة أن ترتب على الدخول تخريب أو إتلاف تشغيل النظام أو تعديل أو محو المعطيات التي يتضمنها النظام بالحبس 3سنوات بدلا عن سنتين وفق قانون 1994 والغرامة 450000الف اورو بدلا عن 200.000 ألف فرنك وفقا لقانون 94 ، وكان هذا التشديد في العقوبة في القانون الجديد دليلا على خطورة تلك الجرائم التي تحتاج إلى مواجهتها بعقوبات رادعة، ويلاحظ بأن قانون العقوبات الفرنسي قد جعل العقوبة أكثر تشديدا من الجزائري، من خلال النص على عقوبة ذات حد واحد لجريمة الدخول والبقاء – في صورتيها العادية أو المشددة- سوى الغرامة أو الحبس بخلاف القانون الجزائري، حيث تضمن=

كما أن التشريع الجزائري قد تأثر بالاتفاقية الدولية للإجرام المعلوماتي - اتفاقية بودابست 2001- والتي أوصت الدول بتضمين تجريم الدخول والبقاء في نظام المعالجة الآلية لمعطيات في قوانينها (1).

وجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات تعد تطوراً أساسيا بالنسبة لقانون المعلوماتية، وقد جعلتها اغلب التشريعات الجريمة الأولى

=حدين للعقوبة سواء في صورتها العادية أم المشددة، وبالتالي فإن القاضي وفقا لـ ق.ع.ف لا تكون لديه سلطة تقديرية بحيث يلتزم في حكمه بذات العقوبة، أما في ق.ج فإن القاضي يتمتع بسلطة تقديرية بين الحد الأدنى والأعلى للعقوبة. ونص المادة (1/323) من ق.ع ف 2004 بالفرنسي:

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d' emprisonnement et de 30000 euros d' amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d' emprisonnement et de 45000 euros d' amende.

(1) تضمنت المادة (2) من اتفاقية بودابست الموقعة في 23 نوفمبر2001 والمتعلقة بالإجرام المعلوماتي على ضرورة تضمين قوانين الدول الموقعة على الاتفاقية، لجريمة الولوج غير القانوني(Illegal access) حيث ورد النص بأنه: (يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا للقانون الداخلي، كما يمكن أن تشترط بأن ترتكب الجريمة من خلال انتهاك الإجراءات الأمنية للحصول على بيانات الحاسب، أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة بحاسب آلي يكون متصلا عن بعد بحاسب آخر، وتقرر المذكرة التفسيرية للاتفاقية بأن الولوج غير القانوني يعد الجريمة الرئيسة التي تنطوي على تهديد، وتعد على أمن النظام، بمعنى السرية والسلامة والإتاحة، إذ أن هناك ضرورة لتوفير حماية ملائمة لمصالح المنظمات، وعلى الأخص لرجال الإدارة حتى يكون بمقدورهم أن يديروا، ويستثمروا، وبناء على ذلك فإن مجرد التداخل غير المصرح به يعني القرصنة (hacking)، أو السطو، أو الدخول غير المشروع في النظام المعلوماتي، كل ذلك يجب اعتباره غير قانوني في حد ذاته كمبدأ عام، وذلك على أساس أن هذه الأفعال يمكن أن تخلق عقبات أمام المستخدمين الشرعيين للنظم والبيانات، كما يمكن أن تؤدي إلى إتلاف أو تدمير باهظ التكلفة في حال إعادة البناء، إضافة إلى أنه يمكن أن يترتب على ذلك الوصول إلى بيانات سرية مثل كلمة المرور أو معلومات عن نظام الهدف وأسرار تسمح باستخدام النظام مجانا، بل وتشجيع القرصنة على ارتكاب أنواع أكثر خطورة من الجرائم المرتبطة بالحاسب مثل الغش المعلوماتي، والتزوير المعلوماتي. ونص المادة بالفرنسي:

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

راجع هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست ألموقعة في23 نوفمبر 2003، مرجع سابق، ص68 وما بعدها، وراجع الموقع الإلكتروني لمكافحة الجريمة الاقتصادية، مرجع سابق، على الرابط:

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm.

بالنسبة لجرائم المعلوماتية، لأنه من خلال الدخول غير المشروع (the admission Illegal) والبقاء يمكن أن ترتكب جرائم معلوماتية أكثر خطورة [1].

كما يلاحظ من خلال نص المادة (394 مكرر) بأن المشرع الجزائري قد جعل لجريمة الدخول والبقاء صورتين مختلفتين.

أ- الجريمة في صورتها العادية

تضمنتها الفقرة الأولى من المادة (394مكرر)، وتخص جريمة الدخول أو البقاء إلى النظام مجردا عن تحقيق أية نتيجة إجرامية، أي أن الجريمة تتحقق بمجرد اقتراف فعل الدخول أو البقاء مجردا عن أي نتيجة [2].

ب- الجريمة في صورتها المشددة

تضمنت هذه الصورة المتمثلة في حدوث نتيجة لجريمة الدخول والبقاء، الفقرة الثانية من المادة (394 مكرر)[3]، فمع أن الأصل في جريمة الدخول والبقاء لا يتطلب لتحقيقها حدوث نتيجة إجرامية، إلا أن الجريمة في صورتها المشددة- وفقا لنص المادة السابقة- يتطلب لقيامها أن تتحقق نتيجة إجرامية تتمثل في حذف أو تغيير المعطيات المخزنة في نظام المعالجة الآلية للمعطيات، أو تخريب النظام، ومع ذلك فإن حدوث هذه النتيجة يتم عن طريق الخطأ وليس العمد، وهذا ما جعل الجريمة في صورتها المشددة المتمثلة بحذف أو تغيير المعطيات المخزنة في نظام المعالجة الآلية للمعطيات تختلف عن الجريمة العمدية للتلاعب بالمعطيات التي نصت عليها المادة (394مكرر1).

أما الجريمة في صورتها الأخرى المتمثلة بجريمة تخريب النظام فإن المشرع الجزائري قد اكتفى بتجريمها كظرف مشدد على جريمة الدخول أو البقاء، ولم ينص على تجريمها في حالة ارتكابها عن طريق العمد أسوة بحذف أو تغيير المعطيات كما في

---

(1) فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية، وخطط التسويق وغيرها، وهذه تمثل هدفا للعديد من الجهات، بما فيها جهات التحقيق الجنائي والمنظمات الإرهابية وجهات المخابرات والأجهزة الأمنية وغيرها، ولا يتوقف نشاط الاختراق على الملفات والأنظمة غير الحكومية بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات قيمة، فعلى سبيل المثال قد يتوصل احد المخترقين للدخول إلى نظام الحجز في أحد الفنادق لسرقة أرقام بطاقات الائتمان، وتتضمن بعض طوائف هذا النمط أنشطة السرقة والاعتداء على الملكية الفكرية كسرقة الأسرار التجارية، وإعادة إنتاج ونسخ المصنفات المحمية، وتحديدا برامج الحاسوب، وفي حالات أخرى فإن أفعال الاختراق التي تستهدف أنظمة المعلومات الخاصة تستهدف منافع تجارية أو إرضاء أطماع شخصية، كما أن الهدف في هذه الطائفة يتضمن أنظمة سجلات طبية وأنظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها.

(2) الفقرة الأولى من المادة (394 مكرر) من القانون رقم (04 – 15) المؤرخ في 10 نوفمبر 2004 المًعدًل و المُتممً للأمر رقم (66-156) المؤرخ 8يونيوسنة 1966 المتضمن قانون العقوبات.

(3)راجع: الفقرة الثانية من المادة(394 مكرر) من نفس القانون .

التشريع الفرنسي، ويعد ذلك قصوراً في التشريع، وفقا لما سيتم إيضاحه أثناء تناول جريمة إفساد أو تخريب النظام.

ويلاحظ من خلال نص المادة السابقة بأن المشرع الجزائري قد استخدم لفظ المنظومة وليس النظام، مما يجعل القارئ للنص يستنتج أو يتبادر إلى ذهنه بأن النظام المحمي جنائيا وفقاً لنص المادة (394 مكرر)، لابد أن يكون عنصرا في منظومة لمعالجة البيانات، لكون لفظ المنظومة قد يشمل أكثر من نظام ، مع أن الهدف من النص هو حماية الأنظمة المعلوماتية التي تعمل منفردة، أو تعمل ضمن منظومة معلوماتية، وكان الأولى أن يكون اللفظ في نص المادة بالنظام وليس المنظومة بحيث تكون صياغة النص (كل من يدخل أو يبقى في نظام للمعالجة الآلية للمعطيات أو يحاول ذلك) لأن النظام لفظ يدخل فيه الدخول إلى نظام بمفرده، أو إلى نظام يعمل ضمن منظومة معلوماتية.

وقد تم تجريم الدخول إلى نظام المعالجة الآلية للمعطيات في أغلب التشريعات في الدول المتقدمة[1] وبعض الدول العربية[2]، وإن اختلفت مابين تشريعات جرمت الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات مجردا عن أي غاية أو هدف، ومنها التشريع الفرنسي والجزائري وغيرهما، وقوانين أخرى جرمت الدخول إلى نظام

([1]) ومن القوانين التي جرمت الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات، القانون البريطاني من خلال نص المادة(5) من القسم(17) من قانون إساءة استخدام الحاسوب البريطاني لعام 1990، وكذلك المادة(1030) من القانون الأمريكي في مجال الإجرام المعلوماتي في التعديل الأخير لعام 2001، والمادة (615) من قانون العقوبات الايطالي، ولفقرة الأولى من المادة(550) من قانون العقوبات البلجيكي، وكذلك المواد (3،4،8،9) من قانون الدخول غير المشروع إلى الحاسوب الياباني رقم (28) لسنة 1999، والمادة(143) من القانون السويسري، لمزيدمن التفصيل راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص129، وص130.

([2]) ومن التشريعات العربية التي نصت على جريمة الدخول غير المشروع، نظام مكافحة الجرائم المعلوماتية السعودي من خلال نص الفقرة (7) من المادة(1) والتي عرفت جريمة الدخول غير المشروع بأنها (دخول شخص بطريقة معتمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها)، وكذلك نصي الفقرتين (2،3) من المادة (3)، والتين تضمنتا تجريم الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا، وكذلك تجريم الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه. كذلك القانون الإماراتي رقم(2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، حيث جرمت المادة(2) منه كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع، أو نظام معلوماتي سواء بدخول الموقع، أو النظام، أو بتجاوز مدخل مصرح به، وشددت العقوبة على جريمة الدخول إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات، كما تم تشديدها بصورة أكبر مما هي عليه في حالة أن ترتكب الأفعال الناتجة عن الدخول من موظف أثناء أو بسبب تأدية عمله أو تسهيل ذلك للغير. كما تضمن تجريم الدخول غير المشروع إلى أنظمة الحاسب الآلي المرسوم السلطاني رقم(72/ 2001) بتعديل بعض أحكام قانون الجزاء العماني من خلال نص الفقرة (2) من المادة (276)، وكذلك قانون العقوبات القطري رقم(11) لسنة 2004، من خلال نص المادة(371) والذي نص على عقوبة كل من توصل بطريق التحايل إلى نظام المعالجة الآلية للبيانات المحفوظة في جهاز حاسب آلي، أو ضبط داخله، أو في أي جزء منه، بدون وجه حق، وتشديد العقوبة بموجب نص المادة (372) في حال أن يترتب على ذلك محو أو تعديل معطيات النظام أو إتلافه، أو تعطيل تشغيله.

المعالجـة الآليـة للمعطيـات واعتبرتـه الجريمـة الأساسـية أمـا بـاقي الاعتـداءات علـى المعطيات والأنظمة المعلوماتية فتعتبر ظروفا مشددةً لجريمـة الدخول ليس إلا، ومنها قانون الولايات المتحدة الأمريكية[1]. وقوانين تتطلب غاية من الدخول إلى النظام كأن يكون ذلك الدخول بغرض تحقيق فائدة أو تخريب لذلك النظام، بمعنى آخر فإن اًعيَدَّن ًن ًن من التشريعات ومنها التشريع الإنجليزي لا يعاقب على عملية الدخول المجرد[2].

2- الركن المادي لجريمة الدخول والبقاء

يقوم السلوك الإجرامي بوصفه عنصرا في الركن المادي للجريمة المعلوماتية على أفعال تختلف عن الأفعال التي يقوم عليها السلوك الإجرامي في الجريمة التقليدية، لأن الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي، ولا يمكن الإمساك بها ماديا [3]، فتقع جريمة الدخول والبقاء بمجرد إتيان النشاط المؤثم، وهو الدخول إلى النظام أو البقاء بعد الدخول بطريقه عرضيه وغير مقصوده[4]، ولذلك فلا يشترط أن تحدث نتيجة مادية معينة، حيث توصف الجريمة بأنها من جرائم الخطر، وليست من جرائم الضرر[5] .

و يشترط لتحقق فعل الدخول أو البقاء أن يتم الدخول، أو البقاء إلى نظام المعالجة الآلية للمعطيات، إذ بدون وجود نظام معالجة آلية لا يمكن أن يتحقق فعل الدخول أو البقاء المجرمين.

كما يشترط البعض لتحقق فعل الدخول والبقاء وجود نظام لحماية البيانات المخزنة في نظام المعالجة الآلية للمعطيات.

لذلك وحتى يتم إيضاح الأفعال التي يقوم عليها الركن المادي للجريمة فسيتم إيضاح مفهوم النظام ومدى تطلب أن يكون النظام محمياً .

---

(1) نائلة محمد فريد قوره، مرجع سابق، ص320.

(2) نائلة محمد فريد قوره، مرجع سابق ، ص320.

(3) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2004، ص115.

(4) هدى حامد قشقوش، مرجع سابق، ص41.

(5) وتعرف جرائم الخطر عند بعض الفقهاء الفرنسيين بأنها الجريمة التي تتضمن تجريم وضع أو سلوك خطر، دون معرفة ما إذا كان سيترتب على ذلك الوضع أو السلوك الخطر نتائج ضاره وفعلية أو لا، وبعبارة أخرى، هي الجريمة التي تتحقق، بصرف النظر عن تحقق النتيجة الضارة. لمزيد من التفصيل راجع علي يوسف حربه: النتيجة الإجرامية دراسة مقارنه، رسالة دكتوراه ، جامعة القاهرة، 1998 ص154 .

أ- مفهوم نظام المعالجة الآلية للمعطيات

لم يورد المشرع الجزائري تعريفاً لنظام المعالجة الآلية للمعطيات، وسار على نهج المشرع الفرنسي بهذا الخصوص، كما لم يتضمن القرار المتعلق بإثراء المصطلحات المعلوماتية تعريفا لنظام المعالجة الآلية للمعطيات رغم أنه يمثل أساس النظرية العامة للقانون المعلوماتي[1]، وبذلك يكون المشرع الجزائري قد وضع في حسابه التطورات السريعة في مجال الحاسوب، والتي قد تضيف مفاهيم أخرى للنظام، وحتى لا يكون ذلك عائقا أمام تلك التطورات في مجال الأنظمة المعلوماتية والتي قد تضاف إليها عناصر أخرى غير تلك التي أوردتها المفاهيم التي عرفت النظام[2].

ب- نظام حماية البيانات

السؤال المطروح الذي سيتم الإجابة عنه من خلال هذا الموضع هو: هل يشترط أن يكون نظام المعالجة الآلية محمياً حماية أمنية- فنية - حتى يتمتع بالحماية الجنائية ؟

وبهذا الخصوص يوجد اتجاهان تناولا هذا الموضوع:

يشترط **الاتجاه الأول** لكي يتمتع النظام بحماية جنائية أن يكون النظام محمياً امنياً [3]، وذلك لعدة أسباب منها:

---

(1) محمد خليفة، مرجع سابق، ص26.

(2) لا يوجد تعريف رسمي لنظام المعالجة الآلية للمعطيات في القوانين الفرنسية المتعاقبة، وبنفس السياق لم يتضمن قانون العقوبات الجزائري تعريفا لنظام المعالجة الآلية للبيانات بخلاف بعض القوانين ومنها قانون العقوبات القطري رقم(11)لسنة 2004 في الفصل الخاص بجرائم الحاسب الآلي، حيث عرف نظام المعالجة الآلية للمعطيات بموجب نص المادة رقم (370) بأنه: (كل مجموعة من واحدة أو أكثر من وحدات المعالجة، سواء تمثلت في ذاكرة الحاسب الآلي، أو برامجه، أو وحدات الإدخال أو الإخراج أو الاتصال التي تسهم في تحقيق نتيجة معينة)، وهذا التعريف مأخوذ من مجلس الشيوخ الفرنسي أثناء مناقشة مشروع قانون 1988 الخاص بجرائم المعلوماتية، إلا أن هذا التعريف لم يؤخذ به في الصياغة النهائية للقانون، وصدر القانون خاليا منه.وكذلك القانون اليمني رقم(40) لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، فقد أورد تعريفا لنظام المعالجة الآلية للمعطيات في المادة الثانية التي تضمنت معاني بعض الكلمات والعبارات، حيث عرفه بأنه: (المنظومة الإلكترونية المستخدمة لإنشاء رسائل البيانات ومعالجتها وتجهيزها وتخزينها وإرسالها واستقبالها)، ويتضح من ذلك بأن القانون اليمني بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية قد أورد تعريفا لنظام المعالجة الآلية للمعلومات، في الوقت الذي لم يتم وضع قانون خاص أو نصوص قانونية لمكافحة الإجرام المعلوماتي يتضمنها قانون العقوبات، و يفترض أن يكون التعريف في ذلك القانون إن لزم الحال، كما يؤخذ على ذلك التعريف أنه عرف النظام بلفظ المنظومة مع أن لفظ المنظومة أشمل وأعم من النظام، كونها قد تشمل أكثر من نظام، وكذلك فإن التعريف قد اقتصر على تعريف النظام من حيث علاقته بأنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.

(3) تنقسم الأنظمة إلى ثلاثة، منها أنظمة مفتوحة للجمهور، وأنظمه قاصرة على أصحاب الحق فيها، وبدون حماية فنية، وأنظمه قاصرة على أصحاب الحق وتتمتع بحماية فنية، والنظام الثالث فقط هو الذي يتمتع بالحماية الجنائية، وفقا للرأي الذي يتطلب شرط أن يكون النظام محميا امنيا حتى يتمتع بالحماية الجنائية، وإذا كان يمكن القول في عدم اشتراط أن يكون النظام المفتوح للجمهور محميا أمنيا لتشابهه مع المحال ألعامة التي يرتادها الجمهور، وينطبق عليها ما ينطبق على المحال العامة، كون تلك الأنظمة متروكة للاستفادة منها للعامة، بخلاف النوع الثاني من الأنظمة وهي التي تقتصر على أصحابها، ولا توجد لها حماية فنية، فلا يشترط أن تتمتع بالحماية الأمنية حتى تتمتع بحماية جنائية، وان كان من الأفضل أن تحاط بالحماية الأمنية كإجراءات وقائية.

- أن القانون لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، وأن من يقوم بالاستغلال عليه أن يستخدم الوسائل اللازمة لمنع الغش، وذلك ما يقتضيه المنطق السليم والعدالة[1]، ومن غير المقبول حماية معلومات مهمة تركها أصحابها والمسئولون عنها دون أية إجراءات تكفل لها الحماية [2].
- أن في ضرورة تطلب الحماية الفنية للنظام يكون بسبب التغيرات والتطور في وسائل الهجوم وأساليبه، والأضرار الناتجة عنه، مما يدفع مستغلي النظم إلى توفير تلك الحماية، ويكون دور القانون الجنائي وقائياً، وذلك ما يتفق مع سياسة المشرع الجنائي، وما يلاحظ من المفهوم العام للحماية الجزائية للملكية [3]، كما أن النظام قد يخترق مع توافر الحماية الأمنية لذلك يجب المراجعة الدورية وتغيير أرقام إدخال المعومات في أجهزة الحاسب الآلي بشكل دوري، وعلى وجه الخصوص أجهزة الحاسب الآلي في البنوك[4].
- أن إقامة الدليل على قيام الركن المادي للجريمة والتحقق من توافر القصد الجنائي لدى فاعلها تتطلب أنظمة أمنية، واختراق هذه الأخيرة يسهل عملية الكشف عن الجريمة، لأنه يترك في العادة أثرا يدل عليه، كما أن الاختراق يساعد في التحقق من القصد الجنائي لدى الفاعل[5].
- يسهل شرط الحماية الفنية التميز بين فعلي الدخول والبقاء كونهما فعلين متميزين فبينما الأول- الدخول – يدخل في عداد الجرائم الوقتية فإن الثاني - البقاء- يدخل في عداد الجرائم المستمرة، وبينما يشترط في الدخول اختراق الأنظمة الأمنية فلا يشترط ذلك في البقاء، لكون البقاء يتطلب أن يكون الدخول متوافقا مع تلك الأنظمة أو أن الدخول قد تم عن طريق الخطأ[6].

---

(1) راجع احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص265 .
(2) نائلة محمد فريد قوره، مرجع سابق ، ص353.
(3) راجع: آمل قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 105.
(4)راجع: محمد سعيد مرهود((جرائم ذوي الياقات البيضاء))، مجلة الحقوق الكويتية،فصلية علمية محكمة، ع3، س23، سبتمبر 1999، ص286.
(5) راجع: أحمد حسام طه تمام، الحماية الجنائية لتكنولوجيا الاتصالات، دار النهضة العربية، القاهرة، 2002، ص2، وراجع:
Xavier Linant de Belle fonds et Alain Hollande . Pratique de l'informatique .4ème édition, Delmas, 1998 , p. 328
مشار إليه لدى: محمد خليفة، مرجع سابق، ص135.
(6) راجع: نائلة عادل محمد فريد قورة، مرجع سابق ، ص354

ومع أن البعض يرى أنه توجد تقنيات حديثة لتامين الأنظمة المعلوماتية من الاختراق ومنها بصمة العين وبصمة اليد بحيث تمثلان نوعا من الدقة في التامين إذا ما تم الجمع بينهما، بحيث يمكن تامين الملفات كلها وعدم فتحها إلا باستخدام تلك التقنية (1)، إلا أن تلك الحماية قد تبدو ضعيفة في حال أن يكون النظام موصل بشبكة المعلومات الدولية، فقد يتم إرسال فيروسات تقوم بتدمير البيانات الموجودة في النظام غير آبهة بتلك الحماية.

بينما لا يشترط البعض(2) -الرأي الغالب- ويسايره القانون الجزائري والفرنسي أن يكون نظام المعالجة محميا أمنيا -فنياً - حتى يتمتع بالحماية الجنائية. ومبررات ذلك الاتجاه:

- أن الحماية الجنائية لا يجوز أن تقتصر على الأنظمة المحمية، و وإنما يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات، سواء كانت تتمتع بحماية فنية أم لا، كون هذا الشرط قد يؤدي إلى الحد من الحماية الجنائية للنظم غير المشمولة بتجهيزات أمنية داخل النظام، ولذلك اكتفى المشرع بأن يكون ارتكاب الجريمة قد تم بطريقة الغش أو التحايل، ويترك تفسير ذلك لقاضي الموضوع في ظل قواعد التفسير وفقاً لمفهوم الأمن المعلوماتي،فمثلاً اشتراط وجود بطاقة تمكن صاحبها من حق الدخول في النظام، فإن التوصل والدخول بكرت مسروق أو مزور يعني الغش والتحايل(3).
- قياس جريمة الدخول غير المصرح به على جريمة السرقة، حيث إن تمتع المال المسروق بحماية صاحبه، وعدم تمتعه لا يؤثر في قيام جريمة السرقة، فالجريمة تقوم، سواء تمتع المال المسروق بحماية صاحبه أم لم يتمتع بها، ونفس الشيء فلا ينبغي لقيام الجريمة أن يكون النظام محميا فنيا**(4)**.
- لم تتضمن النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات في القانون الجزائري وكذلك القانون الفرنسي شرط الحماية الفنية،

(1) Aoughlis Samir, <<Identification Automatique de Personnes à partir de l'Iris de l'œil et de l'Empreinte Digitale >> Mémoire de Magister, Université Mouloud Mammeri, Tizi- Ouzou, Algérie, 2007, p. 88.

(2) راجع: احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص364، ونائلة محمد فريد قورة، مرجع سابق، ص354.

(3)هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، مرجع سابق، ص 28.

(4) راجع: نائلة محمد فريد قورة، مرجع سابق، ص355.

وخرجت خالية منقماماً ، وبالتالي فإنه لا يجوز تقييد النص العام وفقاً للمبادئ العامة المستقرة في القانون الجنائي، وطالما أنه لم يوجد نص خاص يقيد العام فيظل معمولاً بالنص كما هو، ويترتب على ذلك بأن عدم ذكر المشرع لشرط الحماية الفنية يعني أنه أراد استبعاد ذلك الشرط (1).

- أكد القضاء الفرنسي على أنه من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون الفعل قد تم بمخالفة التدابير الأمنية، ويكفي أن يتم الدخول ضد إرادة المسؤول عن النظام (2) .

ونخرج من ذلك بخلاصة نرى من خلالها، أنه لابد أن يتمتع النظام بالحماية الجنائية، ولو لم يكن محمياً أمنيا أو فنيا، فالنظام من الحقوق المملوكة لصاحبها فردا كان أو مؤسسة، والتوصل إلى ذلك النظام أو الدخول فيه يعد انتهاكا لكثير من الحقوق التي تجرمها القوانين التقليدية قبل النصوص أو القوانين المستحدثة، مثل الاعتداء على الحقوق الخاصة، والاعتداء على الأموال المعنوية، إضافة إلى أن أي نظام يتمتع بمزايا وإجراءات قد لا يعرفها إلا المختصون أو الذين لديهم علم بتشغيل النظام، وهذا يعني أن تلك الإجراءات تمثل نوعاً من الحماية الأمنية.

ج- أفعال الدخول والبقاء

يقوم الركن المادي في جريمة الدخول والبقاء على فعل الدخول وفعل البقاء. وبهذا الشأن فقد نص المشرع في المادة (394) من ق.ع.ج على جريمة الدخول والبقاء وأراد أن يفصل بين فعل الدخول وفعل البقاء، حيث يمكن التمييز بينهما بأن فعل الدخول جريمة وقتية، بينما فعل البقاء جريمة مستمرة(3)، وسنتناول كل فعل على حدة .

1) فعل الدخول غير المرخص به أو المحاولة (the unauthorized admission)

يتمثل السلوك الإجرامي لجريمة الدخول غير المرخص به في نظام المعالجة الآلية للمعطيات، بفعل الدخول أو مجرد المحاولة، وفعل الدخول هو سلوك إيجابي من شأنه إحداث تغيير في العالم المعلوماتي بالنسبة لهذه الجريمة وغيرها من الجرائم المعلوماتية.

---

(1) راجع آمل قارة، مرجع سابق، ص 105.
(2) حكم لمحكمة استئناف باريس صادر في عام 1994، راجع نائلة محمد فريد فوره، مرجع سابق، ص355.
(3) احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 281 .

ومحاولة الدخول إلى النظام هو سلوك إيجابي مثله مثل فعل الدخول، إلا أنه يقتصر على المحاولة دون أن يتمكن الجاني من الدخول الفعلي إلى النظام :

أ) فعل الدخول غير المرخص (the admission unauthorized)

تعتبر فكرة الدخول عند البعض فكرة معنوية، باعتبار أن الدخول في نظام معلوماتي هو دخول معنوي[1]. بينما يعتبرها البعض فكرة مادية فيوجد دخول طالما حاول الفرد الدخول أو دخل فعلاً إلى نظام معلوماتي [2].

ووفقاً للنظرية التي تعتبر الدخول فكرة معنوية، باعتبار أنه ليس دخولا في العالم المادي وإنما هو دخول في القدرة على تحقيق عمليات ذهنية أو فكرية، ذلك أن المقاييس أو المعايير التي تحكم العالم المادي لا يمكن تطبيقها على العالم الافتراضي [3] وقد أخذ بهذه النظرية أغلب الفقه الفرنسي، وأخذت بها محكمة استئناف باريس في حكمها الصادر في 5 أبريل 1994.

وقد يكون الدخول إلى نظام المعالجة الآلية للمعطيات دخولاً من حيث المكان عن طريق التسلل إلى داخل النظام المعلوماتي غير المصرح بالدخول إليه، وهو المقصود، وقد يكون دخولاً من حيث الزمان، بتجاوز التصريح المحدد لفترة زمنية محددة،عن طريق تجاوز هذه الفترة الزمنية، والأصل أن يرتبط – تجاوز الفترة الزمنية للدخول- بالبقاء وليس بالدخول [4].

ويتحقق فعل الدخول إلى النظام سواء تم الدخول بشكل كلي أم بصورة جزئية، والحكمة من المساواة بين الولوج الكلي والولوج الجزئي لكون المعتدي في حالة التدخل المقترن بالغش يمكن أن يدعي بسهولة أن تدخله في مكان محدود بجزء ضيق جدا من النظام، ولا يمكن التحقق من هذا الادعاء من الناحية العملية [5].

---

(1)راجع نائلة عادل محمد فريد قورة، مرجع سابق، ص332. وراجع: نهلاء عبد القادر المومني: الجرائم المعلوماتية، رسالة ماجستير، الجامعة الأردنية، ط1، دار الثقافة، عمان،2008، ص158. احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي ، مرجع سابق، ص297.نقلا عن :
Gassin: commentaire de la loi no 88 – 19 – 89 – Précité no 02 in fine commentaire législatif

(2) راجع احمد حسام طه تمام ، المرجع السابق، ص 298.

(3) راجع: محمد خليفة، مرجع سابق، ص142.

(4) احمد حسام طه تمام ، مرجع سابق، ص298م، ومحمد خليفة، مرجع سابق، ص143.

(5)عبدا لله حسين علي محمود، مرجع سابق، ص311.

كما يتحقق الدخول في حالة أن يكون الشخص يعمل من قبل على آله، ثم دخل في نظام أخر عن بعد بفضل الشبكة [1].

وفكرة الدخول في النظام من الناحية الفنية قد ترتكب بوسائل وتقنيات مختلفة[2]، وقد تأخذ أشكالا متعددة، فقد تتمثل بفعل الدخول إلى النظام مع عدم ارتكاب أي فعل

---

(1) نصرون وردية، مرجع سابق، ص14.

(2) **تتعدد وسائل وطرق الدخول إلى النظام المعلوماتي وأكثر الوسائل استخداماً لارتكاب جريمة الدخول غير المشروع هي:**

- **تشغيل كمبيوتر مقفول:** يتم الدخول عن طريق تشغيل كمبيوتر مقفول، وتكون العبرة بالدخول إلى الملفات وليس بالتشغيل، فقد يتمكن المتهم من الدخول إلى الملفات وجهاز الكمبيوتر مقفول، كما انه قد يقوم بتشغيل جهاز مغلق عن طريق توصيله بالكهرباء، ومع ذلك فقد لايتمكن من الدخول إلى الملفات، وعندئذ يعتبر نظام البرمجة مغلقا على الرغم من الجهاز في وضع on بيد انه في الحالة الأخيرة قد حاول الدخول إلى الجهاز، وذلك ما تجرمه بعض القوانين وتساوي بينه وبين جريمة الدخول في العقوبة.
- **استعمال كمبيوتر مفتوح:** وتتمثل هذه الحالة في حالة قيام المتهم باستعمال كمبيوتر كان قيد الاستعمال من قبل صاحبه، مستغلا انشغال صاحب الجهاز، ومن ثم الدخول وفتح ملفات داخل الجهاز، أما إذا اكتفى بالنظر إلى الملفات المفتوحة فلا تتحقق جريمة الدخول.
- **الدخول إلى الكمبيوتر عن طريق بطاقة شخص آخر:** قد يتم الدخول إلى نظام المعالجة لكمبيوتر إحدى الجهات عن طريق (بطاقة) بهدف الحصول على خدمة معينة يقتصر تقديمها على أصحاب تلك البطاقات، سواء تم الحصول عليها عن طريق السرقة، أم العثور عليها بسبب فقدانها، وسواء كان تحمل رقم سري أم أنه يتم الدخول فيها بدون رقم إذا كان النظام يسمح بذلك، وقد يحدث مثل هذا الدخول في حالة سحب مبالغ من البنوك، وقد يتمكن المتهم من الدخول إلى النظام عن طريق العبث بخط التلفون المربوط عليه النظام ويتمكن من الاتصال بنظام من أنظمة الكمبيوتر.
- **الدخول إلى كمبيوتر من كمبيوتر آخر**: قد يتمكن المتهم من الدخول إلى كمبيوتر عن طريق كمبيوتر أخر مع عدم وجود دوائر مشتركة بين الجهازين، وذلك إما عن طريق إجراء توصيلة دون موافقة صاحب الجهاز، أو عن طريق وسائل تقنية حديثة دون إجراء توصيلات، سواء تم ذلك بواسطة برنامج اختراق أم غير ذلك من الوسائل، ومن التطبيقات على ذلك أن يقوم المتهم بالدخول إلى نظام الكمبيوتر لتحويل مبلغ مالي إلى حساب معين، وقد يكون الدخول بغرض الحصول على مكالمات تلفونية مجانية،وتسهل شبكة الإنترنت ارتكاب تلك الجريمة في الدخول إلى الأنظمة التي تتصل بالشبكة، وفي نفس الوقت يكون من الصعب تحديد شخصية المتدخل، حيث يتعمد المتهم الدخول من جهاز إلى جهاز آخر، مرورا بجهاز ثالث، وقد يكون من خارج البلاد.
- **الدخول إلى نظام متصل بنفس الكمبيوتر بدائرة واحدة**: فليس من حق المتهم الدخول إلى نظام من جهازه أو جهاز آخر، وعلى سبيل المثال عندما يشترط الدخول في النظام دفع مبلغ مالي معين، وكذلك عندما يشترط لدخول موقع على الإنترنت أن يكون الدخول ببطاقة مدفوعة الأجر، كما أن بعض المواقع يتطلب الدخول إليها تزويد من يريد الدخول بكلمة مرور من قبل صاحب الموقع، وبالتالي فإن محاولة الدخول أو الدخول إلى الموقع بدون كلمة المرور يكون قد ارتكب فعلا إجراميا.

أما أهم التقنيات فهي :

- **استخدام البرامج المخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة:** على الرغم من ضرورة تزويد الحسابات من بعض أنظمة الحماية الفنية للحيلولة دون الاتصال غير المشروع بالبرامج والبيانات المخزنة، إلا أن إدارة وتشغيل بيانات الحاسبات بطريقة آمنة، خاضعة للتحكم والسيطرة تقتضي وجود نوع من البرامج يمكن استخدامها لتجنب تخطي حواجز الحماية الفنية لمنظومات الحاسب في الحالات الطارئة وحالات اختلال وظائف الحاسب أو توقفها عن العمل.
- **أبواب المصيدة (trap- Doors):** من الأمور الشائعة التي يقوم بها واضعي البرامج ترك فواصل في البرامج أثناء إعدادها تسمى أبواب المصيدة، تستخدم في إضافة ما يحلو لهم من أوجه التلاعب، ويتم ذلك أثناء=

إجرامي آخر، وقد تتمثل بالدخول إلى المكان الموجود به الجهاز، وهذا الدخول لا يمثل جريمة بالمعنى القانوني وفقا لنص المادة (394) من قانون العقوبات الجزائري، وتعد جريمة أخرى هي جريمة انتهاك حرمة مسكن [(1)].

وإذا كان بعض الفقهاء قد اعتبر جريمة الدخول (the admission Crime) جريمة مستمرة، مثلها مثل جريمة البقاء، فإن ذلك يرجع إلى الخلط بين الجريمة وآثارها[(2)]، خاصة أن المشرع قد جرم فعل الدخول في حد ذاته، وبذلك فقد اعتبر فعل الدخول جريمة وقتية، وإلا فلماذا تم تجريم فعل البقاء إضافة إلى فعل الدخول.

ومن ناحية أخرى فإن اعتبار جريمة الدخول جريمة مستمرة، يؤدي إلى عدم إمكانية معاقبة الشخص الذي يدخل بمجرد الصدفة البحتة وبحسن نية، ثم يستمر بعد ذلك في البقاء في النظام المعلوماتي دون وجه حق بعد جريمة الدخول.

ويضم فعل الدخول غير المصرح به (the unauthorized admission) الاختراق (The entering) الذي يحدث للنظام بأكمله أو لجزء منه أياً كان يستوي أن يكون جزاءً مادياً ، أو برامج جزئية، أو بيانات مخزنه في نظام التنصيب،أو فهارس أو بيانات تتعلق بالمحتوى .

= قيامهم بالمعالجة النهائية على اعتبار أن هذا شيء عادي، ويمكن لمهندسي الحاسب أن يقوموا باكتشاف هذا الفاصل من أجزاء داخلية أثناء الصيانة.

- **صناديق القمامة (trash box):** تلقى عادة في سلة المهملات أوراق الكربون أو أوراق عادية تحتوي على بيانات أو حتى أشرطة مغناطيسية من قبل العاملين بواسطة مهندس الصيانة الدورية للأجهزة، وطبيعي لذلك استخدام هذه الملحقات.
- **طريقة (le raccourci):** تمثل هذه التقنية في استغلال نطاق الضعف الخاصة بالنظام الداخلي للرقابة.
- **طريقة القناع :** وذلك بأن يقوم القرصان بإقناع الحاسوب بأنه شخص مرخص له بالدخول.
- **استعمال نقاط الضعف الموجودة على مستوى النظام.** لمزيد من التفصيل في معرفة وسائل وتقنيات الدخول على النظام المعلوماتي راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص315 وما بعدها، وراجع: آمل قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق ص115، ص117، ص118، وراجع أيضا: شيماء عبد الغني محمد عطاء الله، مرجع سابق ، ص129، و محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص102.

(1) يعاقب القانون اليمني على جريمة انتهاك حرمة المسكن وفق نص المادة (253) من قانون العقوبات رقم 12لعام 1994 بالحبس مده لا تزيد عن سنة (1) أو الغرامة من دخل مكانا مسكونا أو معدا للسكن أو أحد ملحقاته أو أي مكان معد لحفظ المال أو عقارا، خلافا لإرادة صاحب الشأن، وفي غير الأحوال المبينة بالقانون، وكذلك من بقي فيه خلافا لإرادة من له الحق في إخراجه، وتكون العقوبة السجن مدة لا تزيد عن خمس سنوات أو الغرامة إذا وقعت الجريمة ليلا أو بواسطة العنف على الأشخاص أو الأشياء أو باستعمال سلاح أو من شخصين وأكثر أو من موظف عام أو ممن ينتحل صفته)، ونص هذه المادة لا يمكن تطبيقه على جريمة الدخول والبقاء إلى النظام المعلوماتي للفرق الشاسع بينهما، فبينما الدخول في نظام معلوماتي هو دخول معنوي فإن الدخول لانتهاك حرمة مسكن هو دخول مادي ملموس.

(2) راجع: احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص203 .

وبالإضافة إلى أن الدخول غير القانوني(the unauthorized admission) يضم الاختراق الذي يحدث للنظام بأكمله أو لجزء منه، فإنه يضم الاختراق الذي يحدث لنظام معلوماتي متصل بنفس الشبكة، أي شبكة محلية أو إنترنت، وفي كل الحالات فإن طريقة الاتصال لا تدخل في الاعتبار، سواء كانت عن بعد أو لاسلكي.

فإذا ما تحقق فعل الدخول أو البقاء إلى نظام معلوماتي، بغض النظر عما إذا كان النظام محميا فنياً أم لا، فإن الجريمة تعد قائمة بمجرد الدخول أو البقاء بدون موافقة صاحب النظام، حتى وإن لم يجد في الملفات ما يبحث عنه من معلومات أو يحدث ضررا[1]، وتؤكد ذلك الفقرة الثانية من المادة (394مكرر) من ق.ع.ج التي شددت العقوبة في حالة حدوث ضرر نتيجة لاقتراف جريمة الدخول أو البقاء في حالة ما إذا نتج -عن الدخول أو البقاء - اعتداء على البيانات المخزنة في نظام المعالجة الآلية للمعطيات، أو على نظام المعلومات.

أخيراً فإنه يشترط في الدخول غير القانوني أن يكون بدون حق، و يكون الدخول بدون حق عندما يقوم الشخص الغير مصرح له بالدخول إلى النظام، مهما كانت الطريقة المستعملة[2]، ومثال ذلك عندما يكون مسموح للشخص بالدخول إلى جزء معين في النظام ولا يحق له الدخول إلى جزء آخر، فدخوله إلى الجزء الغير مسموح له بالنظام يعتبر دخول بدون حق يستحق القمع[3]، وبالتالي فلا تتحقق الجريمة، ولا تكون هناك عقوبة في حالة ما إذا كان الولوج بحق، وذلك في حالة الولوج المصرح به من مالك النظام، أو مالك جزء منه، أو صاحب الحق فيه، كما لا تتحقق الجريمة في حالة ما إذا كان الولوج إلى النظام بالمجان، أو متاحا للجمهور، ففي مثل هذه الحالات يصبح الولوج حقا من الحقوق[4].

---

(1) شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 112.

(2) Jacques Plays: Internet et enquête judiciaire, étude présenté au colloque organisé à Paris les 19 et 20 novembre 2001 par le Ministère de la justice, L'Université Paris I Panthéon Sorbonne et l'Association Arpeje. Sur le droit international de l'internet Sous la direction de Georges Chatillon Bruyant bruxelles 2002, p257.

(3) ومن التطبيقات على ذلك حكم محكمة فرنسية بالسجن خمس سنوات على مستشار لدى إحدى البنوك الكبرى، بسبب قيامة بالدخول إلى المفتاح الثالث في نظام التحويلات الإلكترونية، حيث لم يكن مسموحا له بالدخول إلا إلى مفتاحين فقط – الأول والثاني- ومن ثم قيامه بتحويل 10 مليون$ إلى حساب بنكي فتحه باسمه في بنك في سويسرا. راجع: عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة، الإسكندرية، 2008، ص287.

(4) هلالي عبد ألاه احمد، مرجع سابق، ص72، وص73.

ب) محاولة الدخول إلى النظام

المحاولة بشكل عام إما أن تكون ناقصة أو كاملة، والمحاولة الناقصة هي التي يتوقف فيها تنفيذ الفعل الذي كان الجاني يرغب في تنفيذه، أما المحاولة الكاملة وهي ما يطلق عليها بالشروع في تنفيذ الجريمة، وتتمثل بقيام المتهم بتنفيذ السلوك، إلا أن النتيجة لا تتحقق لظروف خارجة عن إرادته[1].

ومحاولة الدخول إلى نظام المعالجة الآلية للمعطيات، تضمنته المادة (394 مكرر) من ق.ع.ج، وجعلت عقوبة من يرتكب مجرد محاولة الدخول هي نفسها عقوبة فعل الدخول أو البقاء، والهدف من ذلك هو التشديد على حماية الأنظمة المعلوماتية من الانتهاك[2].

وتعد الجريمة قائمة بحق المتهم إذا حاول الدخول إلى نظام الغير للاطلاع على معلومات سرية تخص أفراداً، أو مؤسسات خاصة، أو حكومية، أو بهدف إتلاف البيانات، أو حتى لمجرد محاولة الدخول المجرد، أو لأي هدف كان، إلا أنه لم يتمكن من ذلك، حيث يعتبر في هذه الحالة مرتكبا للجريمة ويعاقب بعقوبتها.

والفرق بين فعل الدخول والمحاولة تكمن في أن السلوك المادي في المحاولة يقتصر على الأفعال التي من شأنها محاولة الدخول، أو القيام بالأعمال التحضيرية التي تعتبر المقدمات لارتكاب جريمة الدخول، ومنها شراء البرامج والأجهزة التي تساعد على الاختراق وفك الشفرات، وبالتالي الدخول على الأنظمة.

أما فعل الدخول فهو الفعل الذي تجاوز مجرد المحاولة بحيث يصل الجاني إلى النظام فعلا، ويصبح بإمكانه التلصص على المعطيات أو إتلافها.

وخلاصة ما سبق فإنه تقع جريمة الدخول من كل إنسان آيا كانت صفته، سواء كان يعمل في مجال الأنظمة أم لا، وسواء كان المتدخل مستعدا لدخوله أم غير مستعد،

([1]) سمير عاليه، شرح قانون العقوبات - القسم العام- دراسة مقارنه، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ص220.

([2]) وقد سار التشريع الجزائري في تجريم محاولة الدخول إلى النظام المعلوماتي على منوال التشريعات الفرنسية المتعاقبة في مجال جرائم المعلوماتية لعام 1988 ،1994، 2004، حيث تكاد نصوص القانون الجزائري تتطابق مع نصوص تلك القوانين، وكذلك القانون الأمريكي لسنة 1994م والذي يعاقب على محاولة استعمال كلمة السر للدخول إلى أجهزة الكمبيوتر الحكومية، وإذا وقعت المحاولة بهدف التأثير على التجارة الخارجية أو التجارة بين الولايات المتحدة، كما أنه يعاقب على استعمال أرقام بطائق الائتمان، أو أي رقم شخصي ينتمي إلى الغير بدون رضاه بغرض الحصول بدون حق على خدمات وأموال . لمزيد من التفصيل حول تجريم محاولة الدخول في القانون الأمريكي راجع شيماء عبد الغني محمد عطاء الله، مرجع سابق، ص140.

فيكفي لتحقق الجريمة أن يكون الجاني قد دخل، أو حاول الدخول إلى النظام مخالفاً شروط الدخول، إذا كان الدخول يستلزم شروطا معينة، أو خالف إرادة من الحق في السيطرة على النظام، كما هو الحال فيما إذا كان القانون يفرض سرية على بعض الأنظمة مثل أسرار الدولة المتعلقة بالمعلومات الذاتية، أو الاسمية، أو أسرار الحياة الخاصة، أو أي معلومات يجمعها الإنسان في النظام ويجعلها لصيقة به، ولا يترك الاطلاع عليها لأي إنسان[1]. كما يكون الدخول غير مشروع إذا كان صاحب الحق في النظام قد وضع كلمة عبور للدخول إلى النظام، ولم يحترم الجاني تلك الكلمة [2]، أو إذا كان يتطلب للدخول دفع مبلغ من المال، وتم الدخول دون دفع ذلك المبلغ[3].

ويتحقق فعل الدخول سواء كان الدخول إلى النظام كله، أو إلى جزء منه، فيكفي أن يتم الدخول إلى بعض عناصر النظام، أو عنصر واحد، أو حتى منطقة ضيقة، طالما أن ذلك العنصر يدخل في برنامج متكامل قابل للتشغيل.

وقد يرتكب المتهم فعل الدخول إلى نظام معين، دون موافقة صاحبه، وفعل آخر يقع تحت طائلة نص عقابي آخر وعندئذ يكون المتهم قد ارتكب جريمتين بينهما ارتباط لا يقبل التجزئة.

([1]) لا يحق لأي شخص الدخول إلى أي نظام للمعالجة الآلية للمعطيات ما لم يكن مرخصا له من صاحب النظام أو من له الحق فيه، إلا أنه تثور مشكلة في حالة تعدد المسؤولين على النظام، وذلك عند وجود أكثر من نظام بحيث تكون تلك الأنظمة نظاما جديدا مملوكا لأكثر من شخص أو أكثر من مؤسسة، وفي هذه الحالة فإنه لابد من تحديد المسؤول على النظام الجديد، وفي حالة عدم تحديد المسؤول عن النظام فان المسؤولية تكون لكل من له حق على النظام الجديد إضافة إلى مسؤولية كلا منهم عن النظام الخاص به، ويترتب على ذلك أن الدخول المصرح به من الذي له حق السيطرة على النظام لا يشكل جريمة دخول غير مشروع، كما تثار مشكلة أخرى في ما إذا كانت تربط بين أكثر من مؤسسه نظام أو أنظمة مشتركه، فهل دخول العاملين الذين يعملون في إحدى هذه المؤسسات يعد دخولا غير شرعي؟ أم أنه ينطبق عليهم الاستعمال غير الشرعي للنظام ؟ وفي مثل هذه الحالة يمكن التفرقة بين ثلاث حالات الأولى: تتعلق بالعاملين بالمؤسسة الغير المصرح لهم بالدخول إلى النظام وهم الذين لا تربطهم بالحاسب الآلي أية صلة وظيفية. والثانية: تتعلق بالعاملين المصرح لهم بالدخول إلى النظام. والثالثة: ترتبط بالعاملين غير المصرح لهم بالدخول إلى النظام إلا أنهم وبحكم مواقعهم بالمؤسسة لديهم من الناحية الفنية إمكانية الدخول إلى النظام، وبالتالي فإن الطائفة التي لا يمكن أن تنطبق عليهم عقوبة الدخول غير المصرح به إلى النظام هي الطائفة الثانية فقط وهم الموظفين المصرح لهم بالدخول إلى النظام. راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص337.

([2]) وتطبيقا لذلك فقد قضت محكمة Douai الفرنسية بوقوع جريمتين من المتهم الذي قام بالدخول إلى نظام الكمبيوتر الخاص بإحدى الشركات ونسخ احد البرامج الموجودة بالجهاز دون موافقة صاحبه، فإنه تتحقق جريمتين الأولى جريمة الدخول في النظام، والثانية الإخلال بحق المؤلف (نسخ البرامج) راجع . شيماء عبد الغني محمد عطاء الله، مرجع سابق، ص141.

([3]) نهلا عبد القادر المومني، مرجع سابق، ص159. ويخالف البعض هذا الرأي - الذي يعتبر أن الدخول بدون دفع الثمن في حال تطلب ذلك من صاحب النظام أو لقائم عليه يعتبر دخول غير شرعي- رأي أخر بحيث لا يعتبر الدخول الذي تم دون دفع الثمن دخول غير شرعي، لكون الحكمة الخاصة بتجريم الدخول والمتمثلة في حماية المعلومات من الوصول إليها، أو حماية خصوصية المعلومات تكون غير متوافرة في حال الدخول دون دفع الثمن، لأن شرط دفع الثمن هو شرط تنظيمي فحسب. راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص336.

وتقع الجريمة بمجرد الدخول إلى النظام مجرداً عن أي نتيجة أخرى، فلا يشترط التقاط المتدخل للمعلومات التي حولها النظام أو بعضها، أو استعمال تلك المعلومات.

ولا تقع الجريمة إذا كان الدخول بحق ولا تكون هناك عقوبة، ومثال ذلك الولوج المصرح به من مالك النظام، أو مالك جزء منه، في حالة أن يكون النظام مملوكا لأكثر من شخص أو مؤسسة، ولم يحدد المسؤول عن النظام أو صاحب الحق فيه، وكذلك في حالة الدخول بهدف اختبار النظام، أو الحماية المصرح بها للنظام محل الشأن.

كما لا تتحقق الجريمة إذا تم الدخول بموجب الالتزام بالشروط التي يفرضها صاحب الحق في النظام أو جزء فيه، كما في حالة الدخول بعد دفع المبلغ المالي المطلوب للدخول، أو كلمة المرور التي يعطيها صاحب الحق في النظام كشرط للدخول إلى النظام، ويعد أيضاً دخولا بحق عدم تجاوز الوقت المصرح به، وكذلك لا تقوم الجريمة في حالة ما إذا كان الولوج إلى النظام بالمجان أو متاحا للجمهور.

2) **فعل البقاء(survival verb)**

يقصد بفعل البقاء " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على النظام" [1].

والبقاء داخل النظام له صور متعددة، منها تجاوز الوقت المسموح به في البقاء داخل النظام، أو البقاء بعد وجود الجاني داخل النظام عن طريق الخطأ وبالصدفة، فقد يجد الشخص نفسه داخل نظام حاسب آلي غير مرخص له بالدخول إليه عن طريق الخطأ مع علمه بذلك، إلا أنه يستمر في البقاء، فيكون بذلك قد ارتكب جريمة بقاء غير مشروع.

ويتحقق االنشاط الإجرامي في نظام المعالجة الإلية للمعطيات في صورة البقاء(the picture survival) داخل النظام، بالتواجد داخل نظام المعالجة الإلية للمعطيات بدون إرادة مالك النظام أو من له حق السيطرة عليه.

([1]) محمد خليفة، مرجع سابق ، ص154 نقلا عن : علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة آليا، مرجع سابق، ص52

كما يتحقق البقاء غير المشروع في النظام في حالة الدخول إلى النظام غفلة، والبقاء فيه، حتى لو لم يتبعه إتلاف للمعطيات (1).

والبقاء داخل النظام لا يختلف عن جريمة الدخول، من حيث وجوب التجريم، فاتجاه إرادة الفاعل للبقاء داخل النظام على الرغم من معرفته بعدم مشروعية البقاء لا يختلف عن الدخول غير المصرح به إلى النظام، فالنتيجة الإجرامية في كلتا الحالتين واحدة، وهي الوصول إلى النظام(2).

وقد يكون فعل البقاء سلبياً وقد يكون إيجابياً، وبالنسبة للفقها الذين يعتبرون الجريمة جريمة امتناع فإن هذه الجريمة تتمثل في عدم توقف الشخص الذي يجد نفسه داخل النظام، رغم علمه بعدم مشروعية فعله(3).أما الذين يعتبرون الجريمة إيجابية فيبررون ذلك بكون الامتناع عن الخروج من النظام بعد الدخول ليس هو محل التجريم، وإنما البقاء غير المصرح به وهو ما يشكل سلوكا ايجابيا (4)

كما يتحقق البقاء غير المشروع في نظر البعض في حالة تجاوز المدة المسموح بها للبقاء في النظام، وفي حالة البقاء في الخدمة أكثر من المقابل الواجب دفعه للخدمة أو الحصول على خدمة دون دفع المقابل(5)، بينما يرى البعض: بأن البقاء بعد تجاوز المدة غير المصرح بها للبقاء في النظام لا تعد جريمة بقاء(6)، لكون الهدف من التجريم إنما هو حماية معلومات وبيانات الحاسب من الاطلاع عليها، وأن البقاء بعد انتهاء المدة المصرح بها لا يحقق ذلك الهدف، كون المعلومات قد تم الاطلاع عليها بداية من التصريح المحدد بمدة زمنية معينة، وإنما يمكن أن تكون الجريمة المرتكبة في هذه الحالة هي جريمة الاستعمال غير المصرح به للنظام.

ومن جانبنا نرجح الرأي الأول على الثاني، لكون تجريم البقاء في نص المادة (394)ع.ج قد جاء عاما، فلم يتضمن التجريم البقاء المشروط بدفع ثمن معين أو مدة زمنية معينة أو البقاء غير المشروط، وجاء شاملا للدخول أو البقاء بشرط أو بدون

---

(1) نصرون وردية، مرجع سابق، ص14.
(2) نائلة محمد فريد فورة، مرجع سابق، ص316
(3) احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي ، مرجع سابق، ص 299.
(4) نائلة محمد فريد فورة، مرجع سابق، ص349
(5) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة ،1-3 مايو 2000، ص 133 .
(6) نائلة عادل محمد فريد قورة، مرجع سابق، ص347

شرط، فإذا ما تحقق البقاء غير المشروع، سواء تم بعد عملية دخول مشروع، أو تم بعد تجاوز المدة المسموح بالبقاء في النظام، أو البقاء مدة تفوق المقابل المطلوب دفعة للبقاء في النظام، فإن جريمة البقاء في النظام تكون قائمة.

أخيرا فقد يتم ارتكاب فعل البقاء مستقلا عن فعل الدخول وقد يجتمعان، إضافة إلى أن فعل البقاء أو الدخول يختلف عن فعل الاعتراض أو الالتقاط وذلك على النحو التالي:

أ) استقلال فعل البقاء عن الدخول واجتماعها

يتحقق فعل البقاء المعاقب عليه مستقلاً عن فعل الدخول إلى النظام، عندما يتم الدخول إلى النظام بصورة مشروعة، ويتحقق ذلك في حالة الدخول إلى النظام عن طريق الخطأ أو بالصدفة، بحيث يجب على المتدخل أن يقطع اتصاله بالنظام فوراً، ومع ذلك يصر على الاستمرار وبالتالي فإنه يعاقب على جريمة البقاء غير المشروع مستقلة عن جريمة الدخول.

ويجتمع فعل الدخول غير المشروع مع فعل البقاء غير المشروع، عندما لا يكون للجاني الحق في الدخول إلى النظام، ومع ذلك يدخل إلى النظام، ولا يقتصر الأمر على ذلك فحسب، بل إنه يظلّ باقياً ومتواجدا في النظام، ويتحقق في هذا الفرض الاجتماع المادي للجرائم (1) .

إلا أن الدخول غير المشروع لا يؤدي حتماً إلى وجود جريمة البقاء غير المشروع، فلا يمكن لجريمتي الدخول والبقاء غير المشروع أن يشكلان تعدداً معنويا للجرائم، حيث إن كل واقعة لها معنى تختلف عن الأخرى (2).

وجريمة الدخول والبقاء تختلف عن بعض الأفعال المتعلقة بالجوانب التقنية في مجال التكنولوجيا الرقمية التي يتم من خلالها سرقة المعلومات، أو الاطلاع عليها أثناء انتقالها من طرفية نظام إلى طرفية نظام آخر، وسيتم إيضاح الخلاف بينها وبين الدخول والبقاء بنوع من الإيجاز.

---

(1) آمل قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 110.

(2) احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص،300.

ب) جريمة الدخول والبقاء و اعتراض والتقاط الرسائل المرسلة

يختلف اعتراض الرسائل التي ترسل عن طريق جهازين كمبيوتر على شبكة مغلقة، أو عن طريق الإنترنت عن جريمة الدخول والبقاء، لكون الالتقاط أو الاعتراض لايتضمن تداخلا في نظام معين ينتمي إلى كمبيوتر معين، ولكنه يمثل نوعا من التلصص على الرسائل المرسلة بين جهازين من الأجهزة، ولا يعتبر من قبيل النشاط الذي يعاقب عليه القانون بوصفه تداخلا، وقد يتم ارتكاب الفعل عن طريق وسائل سلكية تتصل بالنظام أو بطريق التقاط الرسائل بواسطة وسائل حديثة يتم الالتقاط بواسطتها عن بعد[1] حيث يمكن التقاط المعلومات التي يتم نقلها عن طريق الأقمار الصناعية عن طريق وضع أجهزة مطاردة تلتقط المعلومات والإشارات الصادرة عنها في لمحة بصر[2].

وإذا كان يبدو مقبولا التفرقة بين فعل الالتقاط والاعتراض وجريمة الدخول للمبررات السالف ذكرها، وفقا للرأي السابق، فإن ما يؤخذ عليه هو الجمع بين فعل الالتقاط أو الاعتراض بالنسبة للمحادثات التلفونية، فهذه الأخيرة- المحادثات التلفونية- الأولى أن تدخل تحت مفهوم التصنت، كون التصنت لا يتم إلا على شيء مسموع، أما الرسائل فإن كشف محتواها لا يتم إلا عن طريق التقاطها والاطلاع على مضمونها، كما أن لفظ الاعتراض يختلف عن الالتقاط في كون الاعتراض قد يمثل الفعل السابق للالتقاط وقد يهدف إلى ارتكاب فعل أخر، فعن طريق الاعتراض قد يقوم المعترض بالتقاط تلك البيانات وقد يعمل على إتلافها.

وبناء على ما تم ذكره فإنه لا يمكن تجريم فعل الالتقاط للبيانات أو المعلومات المرسلة أو المنقولة بواسطة نظام معلوماتي من خلال نص المادة (394) ق.ع.ج الخاصة بتجريم الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات.

وبالتالي تكون المسألة محسومة ولا تحتاج إلى بحث ما إذا كانت النصوص القانونية الخاصة بالدخول والبقاء يمكن تطبيقها على الالتقاط من عدمه، ويكون القانون الجزائري بذلك قد حذا حذو القوانين الفرنسية الخاصة بمواجهة الإجرام المعلوماتي - سواء قانون 88 أم قانون1994، أم 2004- حيث لم تتضمن جميعها تجريم فعل التقاط المعلومات، بالرغم من أن مشروع القانون الفرنسي لسنة 1988بشأن الجرائم

---

(1) شيماء عبد الغني محمد عطاء الله، مرجع سابق، ص120.
(2) محمد علي العريان، مرجع سابق، ص66.

المعلوماتية في المادة الرابعة كان يجرم كل فعل من شخص يقوم بالالتقاط لبعض المعطيات أو البرامج المسجلة بطريقه عمدية وبدون حق، حيث يلاحظ من خلال النص المقترح التميز بين فكرة الدخول والبقاء عن الالتقاط، من خلال تجريم فعل الالتقاط مستقلا عن فعل الدخول والبقاء[1].

وخلاصة ما تم ذكره فإن ق.ع ج في نصوصه الخاصة بتجريم المساس بأنظمة المعالجة الآلية للمعطيات لم يتضمن نصا قانونيا يجرم فعلي الالتقاط، أو الاعتراض للمعطيات أثناء انتقالها من طرفية إلى أخرى.

كما لا يعاقب عليهما بموجب قوانين التصنت، لذا كان يتعين إيراد نص خاص يعاقب على اعتراض أو التقاط المعطيات، و التصنت على النظام ، لحسم المشكلات القانونية التي قد تظهر بسبب صياغة النصوص التقليدية الخاصة بالمحادثات التي تجري في مكان خاص.

وقد تم تدارك ذلك في بعض الاتفاقيات التي أوجبت على الدول الأطراف فيها، النص على تجريم فعل الالتقاط[2]. و بعض قوانين الدول المتقدمة تكنولوجيا[3].

---

(1) راجع: أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص308، وراجع: شيماء عبد الغني محمد عطاء الله، مرجع سابق، ص120.

(2) ومن تلك الاتفاقيات اتفاقية بودابست حيث تنص المادة (3) منها على (الاعتراض القانوني) وقد ورد النص: (بأنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من اجل اعتبار الاعتراض جريمة جنائية وفقا للقانون الداخلي، واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنيه للإرسال غير العلني، لبيانات الحاسب، في مكان الوصول، في المنشأة أو في داخل النظام المعلوماتي، بما في ذلك الإنبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش) أو أن ترتكب في حاسب آلي يكون متصلا عن بعد بحاسب آخر). والنص بالفرنسي:

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

راجع: الموقع الإلكتروني لمكافحة الجريمة الاقتصادية، مرجع سابق، و احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص308.

(3) ومن تلك التشريعات التي نصت على تجريم فعل الالتقاط التشريع الكندي الذي نص على عقاب كل من يعترض أو يتسبب في اعتراض بدون وجه حق وبسوء نية بأي طريقة كانت، إلكترونية أو ميكانيكية أو سمعيه، أو غيرها بشكل مباشر أو غير مباشر أي وظيفة من وظائف الكمبيوتر. راجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص121 .

كما تضمنت تجريم الالتقاط أو الاعتراض أو التصنت على النظام بعض قوانين الدول العربية [1].

ج) اختلاف فكرة الدخول والبقاء عن استعماله

تختلف فكرة الدخول والبقاء(the admission and survival) في النظام عن استعماله، حيث أن تجريم الدخول والبقاء في النظام لا يعني أن يقوم المتدخل باستعمال الجهاز، كون دائرة الدخول (the admission) أضيق من دائرة الاستعمال (usage)، فكل استعمال للنظام دون رضا صاحبه يشكل دخولا، والعكس فإن الدخول لا يعني بالضرورة استعمال النظام.

فالاستعمال هو كل استخدام الحاسب الآلي ونظامه للاستفادة من الخدمات التي يقدمها دون أن يكون للشخص الذي قام بالاستخدام الحق في ذلك[2].

كما تكمن التفرقة بين الاستعمال والدخول غير المصرح به في كون الأول في الغالب لا يكون إلا من موظفين ينتمون إلى مؤسسة مصرح لهم باستخدام أجهزتها، إلا أنهم يتجاوزون الحق الممنوح لهم في الاستعمال، ويقومون باستعمال الأجهزة لأغراض شخصية، أما الدخول غير المصرح به فقد يتم من أشخاص يعملون في المؤسسة، وقد يتم من أشخاص يعملون خارج المؤسسة.

كذلك فإن الدخول إلى النظام يكون من أشخاص ليس لهم حق الدخول إليه، بعكس الاستعمال الذي غالبا ما يكون من أشخاص لهم حق الاستعمال إلا أنهم يتجاوزن ذلك الحق.

([1]) ومن قوانين الدول العربية التي جرمت التصنت أو الالتقاط أو الاعتراض، القانون الإماراتي رقم (2) لسنة 2006، الخاص بمكافحة جرائم تقنية المعلومات، من خلال نص المادة (8) والتي تضمنت عقوبة الحبس والغرامة لكل من تنصت أو التقط أو اعترض عمداً، من دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، كما تضمنت الفقرة (1) من المادة (3) من نظام مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية، عقوبة السجن مدة لا تزيد على سنة، وغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، لكل من تنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه، كذلك فقد جرم فعل الالتقاط قانون الجزاء العماني، من خلال نص الفقرتين(1، 3) من المادة (276 مكرر) من المرسوم السلطاني رقم(72/ 2001) بشأن تعديل بعض أحكام قانون الجزاء العماني رقم (74/7) حيث تضمن النص على تجريم استخدام الحاسب الآلي عمدا في الالتقاط غير المشروع للمعلومات والبيانات، أو التصنت عليها، وجعل لذلك عقوبة السجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين، والغرامة التي لا تقل عن 100 ريال ولا تزيد عن خمسمائة ريال، أو بإحدى هاتين العقوبتين.

([2]) نائلة محمد فريد قورة، مرجع سابق، ص377.

وبهذا الشأن نود الإشارة إلى أن المشرع اليمني والجزائري لم يتضمن عقوبة للاستعمال غير المشروع للجهاز أو النظام أو الشبكة، ضمن النصوص القانونية الخاصة بتجريم المساس بأنظمة المعالجة الآلية للمعطيات.

3- الركن المعنوي لجريمة الدخول والبقاء

يشترط لتحقق جريمة الدخول والبقاء توافر الركن المعنوي، ويتمثل الركن المعنوي لجريمة الدخول والبقاء في صورتها البسيطة بالقصد الجنائي العام بعنصريه العلم والإرادة، إذ تعد الجريمة في هذه الصورة جريمة عمدية، يجب أن تتم عن طريق الغش، بحيث يتوفر فيها العلم والإرادة [1]، بخلاف الجريمة في صورتها المشددة التي اُعتبرت وفقا لنص المادة(394) ع.ج جريمة غير عمدية.

حيث اشترط المشرع من ناحية أولى أن يكون ارتكاب الجريمة في حالتها الأولى- الدخول المجرد- عن طريق الغش(adulteration) أي جريمة عمدية، ومن ناحية أخرى ضمن عقوبة جريمة التلاعب العمدي في معطيات النظام في نص آخر أشارت إليه المادة (394مكرر1)ع.ج، مما يؤكد أن جريمة الدخول والبقاء في صورتها المشددة- غير المجردة- عندما ينتج عنها التلاعب بالمعطيات أو تخريب النظام جريمة غير عمدية.

أ- الركن المعنوي للجريمة في صورتها البسيطة

يتطلب لقيام جريمة الدخول والبقاء في صورتها البسيطة توافر القصد الجنائي العام بعنصريه العلم والإرادة.

فيجب أن يعلم المتهم بأنه يقوم بالدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات، ولا يهم بعد ذلك أن يتحقق الدخول أو البقاء إلى النظام الذي كان يقصده أم إلى نظام آخر [2] وهذا الفرض على الرغم من أهميته القانونية، إلا أنه يفتقر إلى هذه الأهمية من الناحية العملية، فنادرا ما يدخل الفاعل إلى نظام الحاسب الآلي وهو لا يعلم

---

(1) تصرون وردية ((جريمة الغش في الإعلام الآلي)) ، مطبوعة مقررة على المعد العالي للقضاء، 2001 ، ص14 .

(2) نصت بعض القوانين ومنها قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة على عدم اشتراط أن يكون الدخول إلى نظام محدد بذاته حتى تتحقق الجريمة، إذ نصت المادة 17 منه (على أن التحقق من توافر النية الإجرامية في الدخول غير المصرح به إلى نظام الحاسب الآلي لا ينبغي أن يرتبط بنوعية المعلومات أو البرامج أو الأنظمة محل الجريمة) فالفاعل يسأل عن جريمته ولو لم يكن دخوله مصحوبا بتحديد البرامج والمعلومات التي تم الدخول إليها أو الأنظمة. راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص367.

بذلك، ويرجع ذلك إلى الخبرة التي يتمتع بها مجرم الحاسب الآلي في أغلب الأحوال، التي تحول دون إمكانية التسليم بهذا الفرض، وعلى الرغم من ذلك فإنه إذا ثبت انتفاء هذا العلم انتفى القصد الجنائي[1].

كما يشترط أن يكون الجاني عالماً بأن ليس من حقه الدخول في نظام معلوماتي أو البقاء في ذلك النظام، ولابد أن ينصرف علم الجاني إلى كل واقعة تدخل في جريمة الدخول أو البقاء، فيجب أن يعلم الجاني وهو يرتكب الجريمة بأن فعله ينصب على نظام المعالجة الآلية للمعطيات، وأنه يقترف ذلك الفعل دون ترخيص من مالك النظام أو من له الحق عليه، ويترتب على ذلك انتفاء القصد الجنائي للجريمة في صورتها العمدية في حالة اعتقاد الجاني بأن فعله مبني على تصريح بالدخول أو البقاء، أو أن الموقع الذي قام بالدخول أو البقاء فيه مفتوح للجمهور.

كذلك لا يتوافر القصد إذا كان الدخول عن طريق الصدفة أو السهو أو الخطأ، إلا أنه يتحتم عليه الخروج من النظام بمجرد أن يعلم أن بقاءه في النظام غير مشروع، فإذا لم يقم بالخروج من النظام عقب علمه مباشرة، فإن القصد الجنائي للجريمة يتوافر بحقه ويكون مرتكبا لجريمة البقاء لا الدخول[2].

كما يجب أن يكون المتهم عالما بخطورة الفعل الذي يقوم به - فعل الدخول أو البقاء- وذلك بأن يدرك بأن من شأن ذلك الفعل انتهاك سرية المعطيات المخزنة في النظام، وقد يصل الأمر إلى إتلاف النظام أو المعطيات التي يحتويها.

ويثور التساؤل في تحقق القصد الجنائي حول قيام الفاعل – الذي يعمل غالبا في مجال المعلوماتية – بمحاولة منع خطر يهدد النظام، إلا أنه يترتب على هذه المحاولة الدخول إلى النظام غير المرخص به، فهل يعد ذلك انتفاء للعلم بخطورة الفعل إذ كان يعتقد بأنه لا يترتب على فعله المساس بالحق الذي يحميه القانون وهو الدخول إلى النظام، وبالتالي فإن القصد الجنائي لا يعد متوافرا في هذه الحالة؟ أم أن محاولة منع الخطر الذي يهدد النظام لا علاقة لها بفعل الدخول، وبالتالي فلا يعد مبررا للدخول إلى النظام ؟

([1]) نائلة محمد فريد قورة ، مرجع سابق، ص365.
([2]) محمد خليفة، مرجع سابق، ص164

بهذا الشأن أرجح الرأي القائل بأنه إذا كانت سلطة الفاعل وصلاحيته تسمح له بالدخول إلى النظام، أو إذا كانت القواعد العامة تسمح له بالدخول في حالة الضرورة لمنع الخطر فإنه لا يعد مرتكبا لجريمة الدخول وينتفي القصد الجنائي في هذه الحالة، ولا أتفق معهم بانتفاء القصد الجنائي إذا أقدم على الفعل وهو يعتقد بأنه لن يمس النظام، وسيقتصر فعله على منع الخطر الذي يهدد النظام[1]، لكون فعل الدخول إلى النظام يتحقق في هذه الحالة الأخيرة، طالما لم يخول له القانون منع الأخطار التي تهدد النظام، حيث لا يعقل بأن الجهات أو الأشخاص مالكة النظم لا تنظم مثل هذه المسائل، وتنيط مهام القيام بمنع أي خطر يهدد النظام إلى أشخاص يعملون في تلك النظم، أما قيام شخص أخر غير المكلف بذلك، فإن فعله إذا ترتب عليه الدخول إلى النظام فإنه يدخله في نطاق المسؤولية، لكون الدخول أمر متوقع ومفترض، فمن يقوم بفعل لمنع خطر يهدد النظام لاشك بأنه يتوقع أن يترتب على فعله الدخول إلى النظام.

وإضافة إلى عنصر العلم كعنصر مهم في القصد الجنائي العام لجريمة الدخول أو البقاء، فلابد وأن تتوافر الإرادة، حيث تمثل العنصر الثاني في القصد الجنائي لتلك الجريمة، فالإرادة هي التي تبين الموقف النفسي للجاني حيال السلوك الذي اقترفه، والنتيجة التي تحققت، ففعل الدخول والبقاء يجب أن يتم بالغش، بمعنى أن الفعل يجب أن يكون إراديا وغير مرخص به [2].

ونظرا لكون جريمة الدخول والبقاء من الجرائم الشكلية التي لا تتطلب تحقق نتيجة معينة، فإن الإرادة تقتصر على السلوك الإجرامي وتستغرقه بكل مقوماته، ولا تمتد إلى إي نتيجة، بغض النظر عن الباعث أو الغاية، سواء كان بغرض إثبات وجود ثغرات أمنية في النظام أم بقصد الحصول على أموال الغير أو الانتقام من رب العمل أو صاحب المؤسسة، كل تلك الغايات والبواعث وغيرها لا تؤثر على قيام القصد الجنائي.

وطالما اقتصرت النتيجة في هذه الجريمة على السلوك دون تطلب تحقق الآثار التي يمكن أن تترتب على ذلك، فإنه يجب على الفاعل حتى يتحقق القصد الجنائي أن يتوقع النتيجة المتمثلة بالدخول إلى النظام أو البقاء فيه.

---

(1) نائلة عال محمد فريد قورة، مرجع سابق، ص366

(2) نصرون وردية، مرجع سابق، ص14.

وإذا كان القانون يتطلب أن يكون الدخول إلى النظام قد تم بطريقة غير مشروعة فإنه يثور التساؤل بهذا الشأن حول كيفية التمييز بين الدخول المشروع والدخول غير المشروع؟

وبهذا الصدد فقد اشترط البعض للتمييز بين الدخول المشروع والدخول غير المشروع ،وجود نظام الحماية وهو الذي يضع حداً لكل خلاف حول التفرقة بين الدخول المشروع والدخول غير المشروع، والذي من خلاله يمكن إثبات ومعرفة أن الدخول قد تم بصورة غير مشروعة[1] .

والرأي الراجح هو عدم ضرورة اشتراط انتهاك نظام الأمان كشرط لتوفر الركن المعنوي للجريمة ويساير هذا الرأي التشريع الجزائري والفرنسي.

ب- الركن المعنوي لجريمة الدخول والبقاء في صورتها المشددة

لقد سبق أن أوضحنا أثناء تناول الركن الشرعي لجريمة الدخول في نظام المعالجة الآلية للمعطيات بأن القانون قد جعل لها صورة أخرى مشددة، ونص على تشديد عقوبتها، وذلك في حالتين:

الحالة الأولى: إذا ترتب على الدخول والبقاء حذف أو تغيير لمعطيات النظام.

الحالة الثانية: إذا ترتب على الدخول أو البقاء تخريب نظام اشتغال المنظومة[2].

---

(1) احمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 292 .

(2) وكمثال على الدخول والبقاء غير المشروع إلى نظام المعالجة الآلية للمعطيات إذا استهدف الجاني تخريب نظام اشتغال المنظومة **قضية موريس**، تلك الحادثة التي تعد أحد أول الهجمات الكبيرة والخطرة في بيئة الشبكات، ففي مساء 3 تشرين الثاني عام 1988تمكن طالب يبلغ من العمر 23 سنة ويدعى(Roberts MORRIS روبرت موريس) الذي كان طالبا في مرحلة الدكتوراه (علم الكمبيوتر)بجامعة كور نيل الأمريكية(Cornell University) من إطلاق فيروس عرف باسم (دودة موريس Morris Worm)عبر الإنترنت، أراد أن يثبت عدم ملاءمة الإجراءات الأمنية القائمة لحماية شبكات الكمبيوتر الأمريكية المتصلة مع بعض الجامعات وبعض المؤسسات العسكرية، وقد نتج عن ذلك إصابة وتوقف 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت، من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار، إضافة إلى مبالغ أكثر من ذلك، تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على موريس بالوضع تحت المراقبة لمدة 3 أعوام، ودفع غرامة عشرة آلاف وخمسين دولارا أمريكيا والقيام بعمل لخدمة المجتمع 400 ساعة. لمزيد من التفصيل راجع نائل علي مساعد((أركان الفعل الضار في القانون الأردني))، مجلة دراسات، علمية محكمة، صادرة عن عمادة البحث العلمي بالجامعة الأردنية، ع.1، مايو 2005، ص61، محمود أحمد عبابنة: جرائم الحاسوب وأبعادها الدولية، رسالة ماجستير، الجامعة الاردنية،عمان الأردن، دار الثقافة، 2005، ص103، هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 162، محمود عبد الرحيم الديب، مرجع سابق، ص88.

فلا يشترط أن تكون النتيجة المترتبة على الدخول والبقاء مقصودة، لأن تطلب مثل هذا الشرط غير معقول، لكون المشرع الجزائري نص على تجريم الاعتداء العمدي على المعطيات المدرجة بالنظام بنص مستقل وهو نص المادة(394 مكرر1) ع.ج [1]، وتقابلها نص المادة (323- 1) ع.ف [2].

وعليه فلا يتطلب أن تكون جريمة التلاعب في المعطيات الناتجة عن الدخول والبقاء عمدية، وإنما يكفي أن توجد بين الظرف المشدد وبين الجريمة الأساسية- الدخول والبقاء غير المشروع - علاقة سببية، بحيث تنتفي علاقة السببية إذا أثبت المتدخل أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه لا علاقة لها بفعله المتمثل بالدخول والبقاء، وإنما يعود لسبب خارج عن إرادته مثل الحادث المفاجئ أو القوة القاهرة.

فإذا كان الأصل أن الفاعل لا يقصد أن يتحقق الظرف المشدد كنتيجة لجريمة الدخول والبقاء، فإن القصد الجنائي العام هو المفترض في هذه الصورة، كأثر مترتب على الجريمة، والمسؤولية عن النتيجة المشددة هي مسؤولية غير عمدية تقوم عن طريق الخطأ[3].

ج- مدى تطلب توافر القصد الجنائي الخاص

لا يتطلب ق.ع.ج وبنفس سياق ق.ع.ف توافر القصد الجنائي الخاص في جريمة الدخول أو البقاء غير المرخص بهما، واكتفيا بالقصد الجنائي العام بعنصريه العلم والإرادة لقيام الجريمة.

فلم يتطلب كلا القانونين لتحقق الجريمة أن يكون الهدف إتلاف البيانات أو المعلومات أو أي عنصر آخر، لا يدخل في التكوين العام للجريمة، وإنما يكتفى بتوافر القصد العام لدى الجاني أثناء ارتكاب الجريمة.

كذلك فإن القصد الخاص لا يتحقق في الفقرتين (2،3 من المادة 394 مكرر) ع.ج من خلال النص على الظروف المشددة لعقوبة جريمة الدخول أو البقاء، لكون التشديد في العقوبة ليس عنصرا أساسيا في تحقيق النتيجة.

(1) راجع: المادة (394 مكرر1) من القانون رقم(04 – 15) المؤرخ في 10 نوفمبر 2004.
(2) محمد خليفة، مرجع سابق، ص69.
(3) نصرون وردية، مرجع سابق، ص 14.

فالقانون يجرم الفعل – الدخول أو البقاء – عن طريق الغش سواء ترتبت عليه نتائج أخرى أم لا، إذ إن المشرع تطلب انصراف القصد الجنائي إلى النتيجة الأقل جسامة، وهي الدخول أو البقاء، والاقتصار عليها، ولا عبرة بعد ذلك إن تحققت النتيجة الأشد، كون الفارق بينهما بالعقوبة لا في القصد الجنائي.

وبخلاف عدم تطلب القصد الجنائي الخاص في القانون الجزائري والفرنسي فقد تضمنت بعض القوانين الأجنبية ضرورة توافر القصد الجنائي الخاص في جريمة الدخول والبقاء[1].

كما تضمنت توافر القصد الجنائي الخاص في جريمة الدخول والبقاء إلى جانب القصد الجنائي العام بعض القوانين العربية ومنها القانون السعودي [2].

4- العقوبات المترتبة على جريمة الدخول والبقاء

يتضمن ق.ع.ج نوعين من العقوبات للجرائم الماسة بأنظمة المعالجات الآلية للمعطيات، وهي عقوبات أصلية وعقوبات تكميلية، ولأنه قد تم تناول العقوبات التكميلية أثناء إيضاح الأحكام المشتركة للجرائم المعلوماتية، فسيتم الاقتصار على العقوبات الأصلية لجريمة الدخول والبقاء.

([1]) ومن القوانين الأجنبية التي تطلبت ضرورة توافر القصد الجنائي الخاص في جريمة الدخول والبقاء القانون الدنمركي، حيث يشترط لتشديد عقوبة جريمة الدخول والبقاء أن يكون ارتكاب الفعل بنية الإحاطة بمعلومات تتعلق بعمل إحدى الشركات، أما القانون الاسترالي فقد اشترط للعقاب على جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي نية الإضرار بالغير، والقانون النرويجي يشترط لتجريم الدخول حصول الفاعل له أو لغيره على ربح غير مشروع، أو إلحاق ضرر بالغير، نتيجة الاطلاع على المعلومات، ويشترط القانون البرتغالي في نص المادة رقم (7) من قانون الجرائم المعلوماتية 1991 على عقاب كل من يقوم بالدخول غير المشروع إلى أنظمة وشبكات المعلوماتية أن يكون الدخول بنية الحصول له أو لغيره على فائدة غير مشروعة، وتشدد العقوبة إذا كانت الفائدة أو الربح مرتفعة بصورة كبيرة، أما المادة الثانية من قانون إساءة استخدام الحاسبات الآلية 1990 في المملكة المتحدة فقد تطلبت بجانب جريمة الدخول أن تتوافر لدى الفاعل نية الدخول ونية ارتكاب جريمة أخرى، لمزيد من التفصيل راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص370.

([2]) يستلزم نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) المؤرخ في8/ 3/ 1428هـ، بناء على قرار مجلس الوزراء رقم (79) المؤرخ في 1428/3/7هـ الموافق 26/ 3/ 2007 ، في الركن المعنوي لجريمة الدخول غير المشروع، توافر القصد الجنائي الخاص لدى المتهم بجانب القصد الجنائي العام، حيث يشترط لتحقق الجريمة أن يتم ارتكابها بقصد التأثير في البيانات، أو التأثير في نظام الكمبيوتر نفسه، أو قصد الحصول على بيانات تمس الأمن القومي، أو الاقتصاد الوطني للعقاب ، أو قصد التهديد أو الابتزاز. راجع: شيماء عبد الغني محمد عطاء الله، مكافحة الجرائم المعلوماتية وفقا لنظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، بحث منشور على موقع منتدى كلية الحقوق – جامعة المنصورة، ت.د 2009/8/9 على الرابط:
http://www.f-law.net/law/showthread.php?t=28512
حيث تضمنت القصد الجنائي الخاص في جريمة الدخول: الفقرتان (2، و3) من المادة (3) ، إذ نصت على عقوبة جريمة الدخول بقصد تهديد شخص، أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، حتى لو كان القيام بالفعل أو الامتناع عنه مشروعا، وكذلك الدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم الموقع، أو إتلافه أو تعديله أو شغل عنوانه. راجع موقع جوروسيديا، والموقع السوري للاستشارات والدراسات القانونية، مرجع سابق.

وبهذا الخصوص فقد تضمن ق.ع.ج عقوبتين لجريمة الدخول والبقاء إلى نظام المعالجة الآلية للبيانات في صورتها العادية، وهي الحبس والغرامة، وشدد العقوبات على نفس الجريمة عندما ينتج عند الدخول والبقاء حذف أو تعديل للمعطيات التي احتواها النظام أو تخريب نظام اشتغال المنظومة:

أ- عقوبة جريمة الدخول أو البقاء في صورتها العادية

تكون عقوبة جريمة الدخول والبقاء عن طريق الغش إلى نظام المعالجة الآلية للمعطيات في صورتها العادية الحبس من ثلاثة (3)أشهر إلى (1) سنة، والغرامة من خمسين ألف دينار جزائري إلى مائة ألف دينار (من50.000 إلى 100.000 دج)[1].

ومن خلال العقوبة المشار إليها يتضح بأن المشرع الجزائري قد جعل للقاضي في تقدير عقوبتي الحبس والغرامة حداً ادني وحداً أعلي، حتى يكون له سلطة تقديرية في اختيار العقوبة بحسب الحالة المعروضة عليه، والتي تتناسب مع الباعث والظروف الخاصة بالجاني والجريمة التي تستدعي تطبيق الحد الأدنى أو الأقصى.

---

(1)الفقرة (1) من المادة 394مكرر من (ق.ع.ج رقم (04 - 15)المؤرخ في 10 نوفمبر 2004 ، وقد وردت عدد من النصوص العقابية في عدد من التشريعات العربية تعاقب على جريمة الدخول ومن ذلك نص المادة (276 مكررا) من قانون الجزاء العماني المعدل بموجب المرسوم السلطاني رقم 72 لسنة 2001 ، حيث نصت على أن: (يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين، وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية - فقرة 2- الدخول غير المشروع على أنظمة الحاسب الآلي. وكذلك المادة (371) من قانون العقوبات القطري رقم (11) لسنة 2004 حيث نصت على أن: (يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على عشرة آلاف ريال، أو بإحدى هاتين العقوبتين، كل من توصل بطريق التحايل إلى نظام المعالجة الآلية للبيانات المحفوظة في جهاز حاسب آلي، أو ضبط داخله، أو في أي جزء منه، بدون وجه حق). وكذلك نص المادة (2)من القانون الاتحادي الإماراتي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات حيث نصت على أن: (كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي، سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين). كما نصت المادة (3) في الفقرتين (2، 3)من نظام مكافحة جرائم المعلوماتية السعودي على عقوبة السجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، لكل من يقترف جريمة الدخول إلى النظام بقصد تهديد شخص، أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، وكذلك الدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم الموقع. أو إتلافه أو تعديله أو شغل عنوانه، ونصت المادة(4) فقرة(2)من نفس القانون على عقوبة السجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، لمرتكب جريمة الوصول دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات، وتضمنت المادة (5) فقرة(1) على عقوبة السجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، لجريمة الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها.

ب- عقوبة جريمة الدخول أو البقاء في صورتها المشددة

تشدد عقوبة جريمة الدخول أو البقاء في حالتين، الأولى إذا ترتب على أحد الفعلين -الدخول أو البقاء- حذف أو تعديل لمعطيات النظام، والثانية إذا ترتب عليها تخريب اشتغال نظام المعالجة الآلية للمعطيات [1].

ففي الحالة الأولى -عندما يترتب على جريمة الدخول والبقاء حذف أو تعديل للمعطيات – فإن العقوبة تضاعف على عقوبة جريمة الدخول أو البقاء في صورتها العادية فتصبح ، الحبس من ستة (6) أشهر إلى سنتين والغرامة من مائة ألف إلى مائتي ألف دينار (من 100.000الى200.000 دج).

وفي الحالة الثانية:عندما ينتج عن الدخول والبقاء تخريب نظام اشتغال المنظومة فتكون العقوبة هي الحبس من ستة (6)أشهر إلى (2)سنتين والغرامة التي تتراوح مابين خمسين إلى مائة وخمسين ألف دينار(50.000 إلى 150.000 دج).

ويلاحظ بأن المشرع في هذه الصورة-عندما ينتج عن الدخول أو البقاء تخريب نظام اشتغال المنظومة- قد ضاعف عقوبة السجن على عقوبة الجريمة في صورتها البسيطة، وبذلك تتساوى العقوبة مع الحالة الأولى للجريمة في صورتها المشددة- عندما ينتج عن الدخول التعديل أو المحو للمعطيات، أما عقوبة الغرامة فقد ساوى بين الحد الأدنى للجريمة في صورتها العادية، وبين هذه الصورة حيث جعل عقوبة الحد الأدنى 50.000 دج بينما شدد العقوبة في حدها الأقصى إلى 150.000دج [2].

---

(1) ألفقره الثانية والثالثة من المادة (394 مكرر) من ق.ع.ج رقم(04 - 15) المؤرخ في 10 نوفمبر 2004 ، ومن النصوص في القوانين العربية التي تشدد العقوبة على جريمة الدخول أو البقاء في حالة أن ترتب على الجريمة حذف، أو تعديل المعطيات، أو تخريب النظام نص المادة (372) من قانون العقوبات القطري رقم 11 لسنة 2004 والتي تعاقب بالحبس مدة لا تقل عن سنة، ولا تتجاوز ثلاث سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال، ولا تزيد على خمسين ألف ريال، كل من ارتكب فعلاً من الأفعال المنصوص عليها في المادة السابقة - 371 التي تعاقب على الدخول المجرد- ، إذا نتج عن ذلك محو أو تعديل في المعلومات الموجودة داخل النظام، أو إتلافه، أو تعطيل تشغيله. وكذلك الفقرة الثانية من المادة (2)من القانون الاتحادي الإماراتي رقم (2) بشأن مكافحة جرائم تقنية المعلومات (فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات، فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين).

(2) تدرج قانون العقوبات الفرنسي في رفع عقوبة جريمة الدخول والبقاء في صورتها المشددة وفقا للقوانين المتعاقبة، فقانون 1988 رفع عقوبة الحبس من سنة إلى سنتين، بينما ترك الحد الأدنى للجريمة بصورتيها شهرين، ورفع عقوبة الغرامة في حدها الأدنى والأقصى، وكذلك الشأن في قانون العقوبات لسنة 1994 الذي نص على نفس عقوبة الحبس ورفع عقوبة الغرامة إلى ثلاثين ألف اورو (30.000اورو)، بينما رفعت عقوبة الحبس بموجب قانون العقوبات لعام2004 إلى ثلاث سنوات للجريمة في صورتها المشددة، وسنتين للجريمة البسيطة، كما رفعت الغرامة وفقا للقانون الأخير إلى خمسة وأربعون ألف يورو، ولم يرفع المشرع الفرنسي العقوبة في صورتها المشددة إلى ضعف العقوبة للجريمة البسيطة وفقا للقانون الأخير والاكتفاء برفع العقوبة في صورتها العادية أكثر من القوانين التي سبقته.راجع: محمد خليفة، مرجع سابق، ص174.

5- انعدام جريمة الدخول والبقاء في التشريع اليمني

لم يتضمن القانون العقابي اليمني نصوصاً تجرم فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، سواء ارتكب الفعل بقصد ارتكاب جريمة أم لا، كما أنه لا يوجد نص عقابي في قانون حماية حق المؤلف ينظم هذه الصورة من صور الإجرام، فليست هناك نصوص قانونية تنظم تجريم فعل الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات كجريمة مستحدثة.

وبالرجوع إلى نصوص قانون العقوبات المتعلقة بانتهاك حرمة الحياة الخاصة نجد فيها:

أ- تجريم الاعتداء على حرمة المساكن بنص المادة (253) من قانون العقوبات رقم 12لعام 1994 التي تعاقب بالحبس مدة لا تزيد عن سنة (1) أو بالغرامة لكل من دخل مكانا مسكونا أو معدا للسكن أو إحدى ملحقاته، أو أي محل معدا لحفظ المال، أو أي عقار خلافا لإرادة صاحب الشأن وفي غير الأحوال المبينة بالقانون، وكذلك من بقي فيه خلافا لإرادة من له الحق في إخراجه، وتكون العقوبة السجن مدة لا تزيد عن خمس سنوات أو الغرامة إذا وقعت الجريمة ليلا، أو بواسطة العنف على الأشخاص أو الأشياء، أو باستعمال سلاح، أو من شخصين وأكثر، أو من موظف عام أو ممن ينتحل صفته).

ب- الاعتداء على المحادثات التي تجري بين الأشخاص، أو الالتقاط والنقل للصور وذلك ما نصت عليه المادة (256) ع.ي بالحبس لمدة سنة أو الغرامة لكل من اعتدى على الحياة الخاصة بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا وبغير رضا المجني عليه :

- استراق السمع، أو التسجيل، أو النقل عن طريق جهاز من الأجهزة، أيا كان نوعه لمحادثات جرت في مكان خاص أو عن طريق الهاتف.
- الالتقاط، أو النقل بجهاز من الأجهزة أياً كان نوعه لصورة شخص في مكان خاص.

ومن خلال المواد السالفة الذكر، يلاحظ بأنه لا يمكن تطبيقها على جريمة الدخول والبقاء في نظام المعالجة الآلية للمعطيات لكونها لم تتضمن ما يشير من قريب أو بعيد

على تنظيم ذلك النوع من الإجرام المستحدث، فهي في نص المادة (253) والتي تنظم حرمة الاعتداء على المساكن بمنع دخولها دون إرادة مالكيها، لأن الدخول في الواقع هو دخول مادي ملموس، يتمثل بانتهاك حرمة المسكن، بعكس الدخول في نظام الكمبيوتر، فهو يمثل دخول معنوي تستخدم فيه التقنية الحديثة.

ويبدوا أيضا من ظاهر نص المادة(256) بأنها لا تسري على المحادثات المكتوبة بين جهازين من أجهزة الكمبيوتر، إضافة إلا أن فعلي النقل أو الالتقاط في النص قد اقتصرا على الصورة فحسب وليس البيانات.

وبناء على ما سبق فإن المشرع اليمني لم يجرم فعل الدخول والبقاء في نظام المعالجة الآلية للمعطيات، أسوة بالتشريعات التي سبقته في هذا المجال ومنها في التشريعات العربية التشريع الجزائري والسعودي والقطري والعماني والإماراتي.

ونظرا لما يتطلبه واقع الحال، حيث أصبحت أغلب المعاملات والتعاملات تتم باستخدام النظم المعلوماتية، التي سوف يترتب عليها فيما بعد إما عزل الدول التي لا تواكب ذلك التطور التكنولوجي وهذا ما لم ترتضيه أي دولة تسعى لتحقيق الرفاهية لمجتمعها، أو القبول بالتعايش والتعامل ضمن هذا المجتمع الإلكتروني، بمواكبة التطوير الحادث من ناحية - وهو الخيار الأمثل- ، وإصدار تشريعات أو تعديلها بما تتناسب مع تلك الأوضاع من ناحية ثانية، وأن يستفيد من التشريعات والاتفاقيات الدولية ومنها اتفاقية بودابست ألموقعه في 23نوفمبر 2001م [1].

([1]) وردت من ضمن توصيات اتفاقية بودابست أن على أطراف الاتفاقية أن يتبنوا المدخل العام وأن يقوموا بتجريم القرصنة بلا قيد، أو شرط، وفقا للعبارة الأولى من المادة الثانية من الاتفاقية، كما يمكن لهم أن يحددوا شرطا أو أكثر من الشروط المدرجة في العبارة الثانية من المادة الثانية من الاتفاقية، وذلك باشتراط أن تكون الجريمة ارتكبت انتهاكا لإجراءات الأمن أو نية خاصة تستهدف الحصول على بيانات معلوماتية، أو نية إجرامية أخرى تبرر المسؤولية الجنائية، أو اشتراط أن يتم ارتكاب الجريمة عن طريق نظام معلوماتي متصل عن بعد بنظام آخر، كذلك يمكن حصر الجريمة في الولوج غير القانوني للنظم المعلوماتية على الشبكة، بما في ذلك الشبكات العامة، أو شبكة الإنترنت، أو الإكسترانت التي تعني بالإنجليزية Extra nets ومفردها Extra net ، وهي امتداد شبكة إنترنت بإمكانيات ألشبكه ألعنكبوتيه، (w3) (www) world wide web، والشبكة ألعنكبوتيه: هي خدمة إعلامية واسعة النطاق على المستوى العالمي نشأت على يد SERN في بداية التسعينات وتضم وثائق متشعبة بنظام الديا (الوسائط المتعددة) المتشعبة مخزنة على خدمات البروتوكول http متصلة بشبكة الإنترنت وتسمى هذه الوثائق صفحات ويب web pages وتصاغ بلغة HTML ويمكن الوصول إلى هذه الخدمة عن طريق مميز المصادر (Uniforme Resources locator (URC. راجع: هلالي عبد اللاه أحمد، مرجع سابق، ص76.

وبالتالي فإن عليه - أي المشرع اليمني- أن يصدر تشريعا لمواجهة جرائم المعلوماتية، أو يضمن قانون العقوبات نصوصا قانونية، لمكافحة جرائم المعلوماتية بما فيها جريمة الدخول والبقاء.

وعليه تدارك القصور التي لم يتم تداركها في بعض القوانين، ومنها القانون الجزائري، وذلك بعدم النص على تجريم فعل الالتقاط والاعتراض للمعطيات عن طريق الأنظمة المعلوماتية، لإزالة الالتباس بين فعل الالتقاط والاعتراض وجريمة الدخول والبقاء.

المطلب الثاني

جريمة الاعتداء العمدي على البيانات المخزنة في النظام

تعد جريمة التلاعب بالمعطيات المخزنة في نظام المعالجة الآلية إحدى الجرائم المعلوماتية المستحثة التي ظهرت بظهور التكنولوجيا الرقمية، لما لتلك التكنولوجيا من دور هام في تخزين الكم الهائل من المعلومات.

وقد زادت أهمية تلك المعلومات في هذا العصر الذي أطلق عليه بعصر المعلومات، كونها أصبحت بمثابة المادة الخام التي يقوم عليها التطور الحادث في شتى مجالات الحياة المختلفة، حتى أطلق عليها بالبترول الرمادي، بحيث يمكن القول بأن من يمتلك الكم الهائل من المعلومات، بلا شك يمتلك حضارة يتفوق بها عن من هو أقل منه في امتلاكها.

ولما للمعلومات من أهمية في صناعة التطور التكنولوجي، وما يترتب عليه من تطورات في شتى المجالات المختلفة، حيث أصبحت سلعة تباع وتشترى، تتسابق الدول لاقتنائها، كما أنها تعد أساس عمل النظام المعلوماتي، فقد أضحت محلا للاعتداء عليها بحذفها أو تغييرها أو إتلافها، لذلك فقد اهتمت التشريعات والمؤتمرات والاتفاقيات الدولية بتجريم الاعتداءات التي تستهدفها، ومن تلك الاتفاقيات اتفاقية بودابست[1].

([1]) اوجب نص المادة (4) من اتفاقية بودابست الموقعة في 23نوفمبر 20001م على الدول الأطراف في الاتفاقية تبني الإجراءات التشريعية وأية إجراءات أخرى ترى كلا من تلك الدول أنها ضرورية للتجريم، تبعا لقانونه المحلي، إذا حدث ذلك عمدا، ودون حق ، أي إضرار، أو محو، أو تعطيل، أو إتلاف، أو طمس لبيانات=

لما تم ذكره فسنتناول الجرائم التي تمس المعطيات المخزنة بنظم المعالجة الآلية، سواء تمثلت بإدخال أو تعديل أو حذف معلومات في نظام معلوماتي بصورة غير مشروعة، وكذلك الأركان المكونة لها والعقوبات المترتبة عليها.

1- الركن الشرعي لجريمة التلاعب العمدي بالبيانات المخزنة بالنظام

يتمثل الركن الشرعي لجريمة الاعتداءات العمدية لمعلومات مدرجة بالنظام المعلوماتي في القانون الجزائري بنص المادة (394 مكرر1)، حيث نصت على أنه **(**يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال، أو عدل بطريق الغش المعطيات التي يتضمنها **)** (1)، وقد ساير القانون الجزائري بذلك القانون الفرنسي.

=الحاسب، ويمكن لأي طرف أن يحتفظ باشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة.

ونص المادة بالفرنسي:

Article 4 – Atteinte à l'intégrité des données

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
2. 2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

وراجع هلالي عبد اللاه أحمد، الجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص58.

(1) المادة (394 مكرر 1) من القانون الجزائري (رقم 04 – 15) المؤرخ في 10 نوفمبر 2004 ، ونص المادة بالفرنسي:

Est puni d'un emprisonnement de six (6) mois a trois (3) ans et d'une amende de 500.000 DA à 2.000.000 de DA, quiconque introduit frauduleusement des données dans un système de traitement automatisé ou supprime ou modifie frauduleusement les données qu'il contient .

وتقابلها نص المادة (323 / 3) من قانون العقوبات الفرنسي لعام94، وهي نفس المادة في القانون المعدل لعام 2004 إلا أن العقوبة قد تم تشديدها وفقا للنص الجديد، فأصبحت عقوبة الحبس خمس سنوات بدلا من ثلاث، والغرامة 75 ألف يورو بدلا من 45 ألف يورو وفق النص السابق في قانون 94. ونص المادة بالفرنسي:

Article 323-3

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 III Journal Officiel du 22 juin 2004)

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

كذلك فقد تضمنت بعض القوانين العربية تجريم الاعتداءات العمدية على المعطيات المخزنة بنظم المعالجة الآلية للمعطيات[1].

وبالمقابل فلم يتضمن القانون اليمني نصا قانونيا ينص على جريمة التلاعب بمعطيات الحاسوب، ولا يمكن تطبيق النصوص التقليدية الخاصة بجريمة التزوير، لكون تلك النصوص تعالج تزوير المحررات الرسمية وغير الرسمية، في مستندات مادية مكتوبة بخلاف التزوير بالمستندات المعلوماتية، حيث يمكن تزويرها في نظم المعالجة الآلية للمعطيات، كما يمكن تزويرها بعد أخراجها من النظم، وهي تختلف عن التلاعب في المعطيات المخزنة بنظام الحاسوب والتي تتطلب دائما تزويرها إثناء بقاءها ومعالجتها بالنظام، ومن ثم تحتاج إلى مواجهتها بنص مستحدث[2].

ويتضح من خلال النص الذي يجرم الاعتداءات العمدية على المعلومات المدرجة بالنظام، بأن المشرع الجزائري قد سار على نهج المشرع الفرنسي، وتوسع في تجريم الدخول إلى أنظمة المعالجة الآلية للمعطيات، بغرض الاعتداء على المعطيات المدرجة

(1) سايرت عدد من التشريعات العربية القوانين الحديثة في تجريم الاعتداءات العمدية على المعطيات المخزنة بنظم المعالجة الآلية للمعطيات، حيث جرمها قانون الجزاء العماني بموجب نصي الفقرتين(6 ،9) من المادة (276مكرراً)، إذ تضمنت الفقرة(6) تجريم استخدام الحاسب الآلي في إتلاف، وتغيير، ومحو البيانات والمعلومات، بينما تضمنت الفقرة(9) تجريم التعدي على برامج الحاسب الآلي بالتعديل، أو الاصطناع . كذلك فقد تضمنت الماد (373) من قانون العقوبات القطري رقم (11) لسنة، 1994 ، تجريم الإدخال عمداً، سواء بطريق مباشر أو غير مباشر، بيانات في نظام المعالجة الآلية الخاص بشخص أو بجهة ما، أو تدمير، أو تعديل البيانات التي يحتويها، أو طريقة معالجتها، أو نقلها. وتضمنت المادة(6) من القانون الإماراتي بشأن مكافحة جرائم تقنية المعلومات تجريم إدخال عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه تدمير، أو مسح، أو حذف، أو إتلاف، أو تعديل البرامج، أو البيانات، أو المعلومات، كما جرمت المادة(7) من ذات القانون تعديل، أو أتلاف الفحوص الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو تسهيل ذلك للغير، أو تمكينه من ذلك، باستعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. أخيرا فقد جرم نظام مكافحة الجرائم المعلوماتية السعودي من خلال نصي الفقرتين (1، 2) من المادة(5) الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها، وكذلك تدمير أو مسح البرامج، أو البيانات الموجودة في الشبكة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

(2) نص المشرع اليمني على جرائم التزوير في المواد (من 204 إلى 219) ضمن الباب الثامن في فصلين تضمن الفصل الأول تزييف النقود والطوابع والأختام الرسمية، وفي الفصل الثاني تزييف المحررات رسمية كانت أو غير رسمية، حيث يلاحظ على تلك النصوص أنها تتعلق بجريمة التزوير والتزييف التقليدية، التي تتم في الأوراق والمحررات المكتوبة، وقد تنطبق تلك النصوص على جرائم التزوير والتزييف إذا ما تم ارتكابها بواسطة نظم المعلوماتية وتم إخراجها بصورة مادية ملموسة، أي بعد طباعتها، باعتبار أن نظم المعلوماتية ما هي إلا وسائل لارتكاب تلك الجرائم، إلا أن تطبيق تلك النصوص لا تتناسب مع الجريمة بصورتها المعلوماتية، عندما تكون مخزنة بنظم المعالجة الآلية للمعطيات قبل أن تتخذ شكل المحرر الإلكتروني، لما قد يترتب عليها من معاملات بوصفها الإلكتروني، إذ لايتطلب أن يتم أخراجها بصورة مطبوعات، فلقد أصبحت أغلب التعاملات تتم عن طريق المعطيات والوسائط المخزنة لها، فهي في هذه الحالة تمثل كيانات منطقية، تتم من خلال التلاعب بالمعطيات التي ينتج عنها معطيات غير أصلية، كذلك لا يمكن تطبيق النصوص التقليدية على تزوير المعلومات المسجلة كهرومغناطيسيا على وسائط التخزين الخاصة بها، حيث لا يمكن مشاهدة تلك المعلومات عن طريق النظر المباشر، كونها تفتقر إلى صفة المحرر، وبالتالي فإن على المشرع اليمني تعديل النصوص القانونية الخاصة بجريمة التزوير لتشمل التزوير المعلوماتي.

بالنظام، سواء تمثل ذلك الاعتداء بإدخال معطيات، أو إلغائها، أو تعديلها، نظرا لخطورة تلك الأفعال على المعلومات، وما تمثله من قيم يترتب على الاعتداء عليها بالإلغاء، أو المحو، أو التعديل أضرار بالغة على مستوى الأفراد، أو المجتمعات، أو حتى اقتصاد وأمن الدول بحسب ما إذا كانت المعلومات تهم فردا بعينه، أو مجتمع بذاته، أو دولة بسيادتها.

وتجدر الإشارة إلى أن الحماية الجنائية التي يوفرها النص تقتصر على المعطيات المخزنة في نظام الحاسوب طالما أنها تدخل في نظام المعالجة الآلية للمعطيات وتشكل وحدة واحدة من عناصر النظام، ويترتب على ذلك أن هذا النص لا يتناول بالحماية المعطيات التي خارج النظام، حيث تناول حمايتها نص أخر هو نص المادة (394مكرر2).

وقد يتبادر إلى الذهن بأن نص المادة (394 مكرر1)، المتعلقة بإدخال أو تعديل أو محو البيانات تعالج مسألة تزوير مستندات المعالجة الآلية، لأن المادة تتحدث عن التغيير في البيانات وبالتالي المستندات.

وذلك أمر منتقد لان البيانات المسجلة في الحاسوب تعد مخزنة بداخل النظام، أما المستند المعالج آليا فقد يكون بداخل النظام وقد يكون بخارجه وفي الحالتين يمكن أن يخضع للتزوير، وبالتالي فلا يمكن القول بخضوع المستند إذا كان خارج النظام للنصوص التقليدية لجريمة التزوير، وتطبيق النص المستحدث على تزوير المستندات أو البيانات المخزنة في النظام [1].

ويترتب على ما سبق عدم إمكانية تطبيق نص المادة (394 مكرر1) ع.ج على جريمة التزوير المعلوماتي، حيث مازال القانون الجزائري في تعديلاته التي تمت في 2004، و2006، 2009، لم يتضمنها، بالرغم من أهميتها.

وعلى المشرع الجزائري واليمني إعادة النظر في ذلك وتجريم تزوير المعطيات المخزنة في نظام المعالجة الآلية للمعطيات، والمستندات المعالجة معلوماتيا، شريطة أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف

([1])راجع: هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، مرجع سابق، ص124.

أو أن يصلح لإثبات حق أو تصرف له آثار قانونية، مثلما فعل المشرع الفرنسي[1]، وبعض التشريعات العربية [2].

ونظرا لأهمية جريمة التزوير المعلوماتي وتشعبها ولعدم تناول القانون الجزائري واليمني لها فقد يأتي الحديث عنها في دراسات قادمة مع ما تبقى من الجرائم المعلوماتية.

2- الركن المادي

يتمثل الركن المادي في جريمة الاعتداء ألعمدي على المعطيات في إحدى الصور الثلاث التالية :

أ- الإدخال (input)
ب- المحو (erasure)
ج- التعديل (Alteration)

وسنوضح هذه الأفعال-الصور- بالتفصيل فيما يلي :

أ- الإدخال : (input)

ويقصد بفعل الإدخال(input) إضافة معلومات جديدة على الدعامة سواء كانت خالية من المعلومات أم كان يوجد بها معطيات.

---

(1) حسم المشرع الفرنسي الجدل في قانون العقوبات منذ عام 1994حول مدى انطباق النصوص التقليدية الخاصة بالتزوير على التزوير المعلوماتي، من خلال نص المادة (1/441) التي توسعت في مفهوم المحرر الذي يقع عليه التزوير، بحيث أصبح التزوير يشمل بجانب المحرر المكتوب، كل وسيط آخر للتعبير عن فكرة، مثل الأقراص الممغنطة والاسطوانات المدمجة وغيرها من وسائط التخزين المعلوماتي، والنص بالفرنسي:

Article 441-1

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende.

في مضمون المادة بالعربي راجع: نهلاء عبد القادر المومني، مرجع سابق، ص150. وفي النص الفرنسي راجع: http://www.unhcr.org/refworld/country,,NATLEGBOD,,COD,456d621e2,47303b9e2,0.html

(2) تضمن قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم(2) لسنة 2006، تجريم تزوير المستندات المعلوماتية من خلال نص المادة (4) منه حيث نصت على أن (يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفاً به قانوناً في نظام معلوماتي. وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر، ويعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه)، وتضمنت المادة (380) من قانون العقوبات القطري رقم (11) لسنة 2004 على جريمة التزوير المعلوماتي، حيث نصت على أن (يعاقب بالحبس مدة لا تجاوز خمس سنوات، كل شخص ارتكب تزويراً في المستندات المعالجة آلياً، أياً كان شكلها، إذا ترتب عليه الإضرار بالغير، أو استعمل هذه المستندات المزورة مع علمه بذلك، ويعد تزويراً كل تغيير في برامج الحاسب الآلي، أو البرامج المسجلة على ذاكرته، للحصول على نتائج غير صحيحة)، كما نصت الفقرة(5) من المادة (276) قانون الجزاء العماني 2001 على تجريم تزوير بيانات أو وثائق مبرمجة أيا كان شكلها، وجعلت عقوبة ذلك السجن مدة لاتقل عن شهرين ولاتزيد عن سنتين، والغرامة التي لاتقل عن مائة ريال ولاتزيد عن خمسمائة ريال.

وإدخال بيانات غير معتمدة في نظام معلومات الحاسب أو تحريف البيانات المعتمدة المراد إدخالها تعد من أكثر أساليب ارتكاب الاحتيال المعلوماتي أمنا، وأكثر أشكاله وقوعاً، حيث يشكل ما يقع باستخدامه أكثر من نصف إجمالي حالات الاحتيال المعلوماتي[1].

ويتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان، سواء ارتكب ذلك الفعل من صاحب البطاقة الشرعي، أو من غيره في حالة سرقتها وفقدانها أو تزويرها.

كما يمكن أن يتم فعل الإدخال في كل حاله يتم فيها إدخال برنامج غريب فيروس أيا كان ذلك النوع من الفيروسات، حصان طروادة، أو قنبلة معلوماتية، أو نوع من أنواع الديدان.

وقد يكون الهدف من فعل الإدخال إتلاف البيانات المخزنة بالنظام، أو تعديل معلومات معينه تتعلق بالجانب المالي لأموال مودعه في البنوك [2].

ب- المحو : (erasure)

يقصد بالمحو أو الإزالة: اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو طمسها، وكذلك عن طريق تحويل خصائص مزالة في منطقة محفوظة من الذاكرة[3].

كذلك يقصد به: إزالة جزء من المعطيات المسجلة على دعامة أو الموجودة بداخل النظام، أو تحطيم تلك الدعامة، أو نقل أو تخريب جزء من المعطيات إلى المنطقة

(1) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 59.

(2) فقد أصدرت محكمة L,eeds crown court عام 1983،حكما بحبس طومسون Michal Thompson- والذي كان يعمل خبيرا في بنك الكويت التجاري، خمسة عشر شهر بسبب استيلائه على بعض الأموال المودعة في بنك الكويت التجاري، وملخص وقائع القضية قيام الخبير طومسون أثناء تعديل برنامج التحويلات في البنك واستغلال سفر المشرف عليه إلى باكستان، بإدخال برنامج يقوم بتحويل أموال من أرصدة خمسة من المستثمرين الكويتيين عبر عدد من فروع البنك إلى رصيد قام بفتحه باسمه، وكان من ضمن الأوامر المدخلة بالبرنامج تحديد وقت قيام النظام بإجراء عملية التحويل أثناء ما يكون على متن الطائرة المتجهة إلى لندن، بعد أن انتهت فترة عمله بالبنك الكويتي، وتمت عملية التحويل، وفور وصوله إلى لندن قام بطلب تحويل المبالغ المالية من رصيده في الكويت إلى بنك في لندن وتمت عملية التحويل وكشف أمره، و تمت محاكمته على ذمة إدخال بيانات غير صحيحة إلى نظام المعالجة الآلية للمعطيات، وتحويل أموال وفق القانون البريطاني، مع أنه قد دفع بعدم اختصاص القضاء البريطاني بنظر جريمة لم ترتكب على أراضيه، حيث لم يقبل ذلك الدفع لكون آخر عملية للجريمة ارتكبت من بريطانيا، وهي عملية تحويل الأموال من الكويت إلى بريطانيا. راجع: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 80.

(3) محمد خليفة، مرجع سابق، ص157،وهو تعريف للفقيه الفرنسي (Buffelan).

الخاصـة بالـذاكرة، ومـع أن التعريـف يـدل علـى أن المحـو يعنـي الإتـلاف إلا أن بعـض التطبيقات القضائية اعتبرتها جريمة نصب [1].

وأحيانا قد تكيف واقعة إتلاف الوثيقة المعالجة آليا إذا ما تم محوها أو تعديلها على أنها تزوير، مع أنها في الحقيقة واقعة إتلاف، كون التزوير يشترط أن تكون الوثيقة مكتوبـة، كما أن التغير أو التعديل علـى الوثيقـة المعالجـة يغير مضمونها، ويجعل لها معنى مغايرا لما كانت عليه من قبل، وتعتبر الوثيقة الأصلية أتلفت بموجب التعديل الذي طرأ عليها[2].

وفعل الإزالـة يـأتي بعد فعل الإدخـال، إذ لا يعقل أن يـتم إزالـة معطيـات لـم يـتم إدخالها من قبل [3].

ج- التعديل : (Alteration)

يقصد بتعديل المعطيات: تغيير المعطيات الموجودة داخل نظام المعالجة الآلية للبيانات أو استبدالها بمعطيات أخرى. كما يقصد بـه قيام الغير ممن لا يملك الحق في إحداث تعديل في المعلومات بتعديلها [4].

([1]) ومن ذلك تكييف ما قام به متهم محاسب بإحدى الشركات بعد ستة شهور من بداية العمل، بمحو بيانات ومعلومات معالجة آليا، تخص إحدى الشركات على أنه نصب، بالرغم من أن ذلك يشكل جريمة إتلاف للمعلومات عن طريق المحو، والمحو وسيله من وسائل الإتلاف، وهذا يعني أن المحو الذي وقع عن طريق الاعتداء على المعطيات المدرجة بالنظام أو بالبرنامج المحاسبي للشركة قد كيف جنائيا على أنه نصب بالرغم من أن المحو من وسائل الإتلاف. راجع:

Voir Dvleray R. et Rocco A.M. les escrocs a l' informatique, le nouvel Economiste, l'er oct. 1979.

مشار إليه لدى أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص356 .

([2]) اعتبرت محكمة النقض الفرنسية تعديل المعطيات التي يتضمنها النظام جريمة إتلاف وليست تزوير بناء على قرارها في 8 ديسمبر 1999بخصوص تعديل أو إلغاء عمدا بالمخالفة للوائح المطبقة لمعطيات يحتوي عليها نظام معالجة آلية، حيث أقرت أنه ليس من اللازم أن تكون هذه التعديلات أو الإلغاءات قد تم ارتكابها بواسطة شخص ليس له حق الدخول إلى النظام، ولا يشترط حتى أن يكون لديه نية الإضرار، ومن خلال ذلك يلاحظ بأن المحكمة الفرنسية قد اعتبرت أن الواقعة واقعة إتلاف وليست جريمة تزوير، لكون التزوير يشترط أن يكون بنية الإضرار. مشار إليه في مؤلف احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص،357، وص358.

([3]) ومثال للقضايا التي تتعلق بفعل الإزالة أو المحو "قضية شركة (TRW company Credit data) الأمريكية التي تعمل على تزويد عملائها بمعلومات من خلال حاسباتها الآلية تتعلق بالمركز الائتماني لأفراد الجمهور نظير اشتراك يدفعه العملاء للشركة، وكانت الشركة تضم في أنظمة حاسباتها معطيات تتعلق بحوالي خمسين مليون شخص، وقد استغل ذلك أحد العاملين بالشركة بقسم علاقات المستهلكين، وقام ببيع مراكز ائتمان جديدة قام هو باختلاقها لأصحاب مراكز ائتمانية رديئة مقابل مبلغ من المال يدفعه هؤلاء، حيث قام بمحو المعطيات المتعلقة بالمراكز الائتمانية الرديئة واستبدالها بمراكز ائتمانية أخرى بحسب المعطيات التي يمليها عليه أصحاب تلك المراكز، وكانت نتيجة ذلك أن تورط العديد من عملاء الشركة بالتعامل مع أصحاب مراكز ائتمانية رديئة بموجب المعلومات الخاطئة التي قدمت لهم. راجع محمد خليفة، مرجع سابق، ص184، وص185.

([4])عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص.363.

وقد تضمنت المادة(394 مكرر 2).ع.ج، فعل التعديل والعقوبة المترتبة عليه، إضافة إلى فعلي الإدخال والإزالة [1]،لأن هذه الأفعال الثلاثة تمثل جريمة التلاعب في المعطيات المخزنة بنظام المعالجة الآلية للبيانات، فتجعل تلك البيانات مختلفة في الهدف والغاية عن البيانات التي كانت مخزنة في النظام، فالهدف من الأولى – البيانات بعد الإدخال، أو الإزالة، أو التعديل- غير مشروع ، ومن الثانية - البيانات الأصلية- مشروع.

ويختلف فعل التعديل عن فعل الإدخال في كون التعديل يتضمن التغيير في البيانات المخزنة في النظام، أما الإدخال فقد يتم بإدخال بيانات إلى نظام خال من البيانات، وقد يتم إدخال بيانات إلى البيانات الموجودة في النظام، كما يختلف فعل التعديل عن فعل الإزالة في كون الأول - التعديل- يتضمن تغييرا في البيانات الموجودة أصلا في النظام، أما الثاني – الإزالة- فيتضمن إزالة ومحو البيانات الموجودة.

وتعديل المعطيات المخزنة في نظام المعالجة الآلية للمعطيات قد يشمل تعديل المعطيات فقط، وقد يشمل تعديل البرامج.

فالتلاعب في المعطيات بتعديلها تتحقق إما في مرحلة الإدخال[2]، أو في مرحلة الإخراج، وهي المرحلة التالية لإعطاء الأمر بإخراج المعطيات والسابقة على عملية الإخراج [3]، إلا أن هذه المرحلة وفق هذا الرأي لا يمكن من خلالها أن يتم تعديل المعطيات لكون المعلومات بعد إعطاء الأمر بإخراجها تخرج عن سيطرة من يريد إجراء التعديل عليها، ولا يبقى لنظام المعالجة دور في التعديل بحيث تصبح المعلومات في هذه الحالة خارجة من نظام المعالجة الآلية للمعطيات، ولا يمكن تطبيق النص القانوني لجريمة التلاعب في المعطيات المخزنة في نظام المعالجة الآلية للمعطيات على هذه الحالة.

---

(1) المادة (394 مكرر 1) من ق .ع.ج رقم (04 – 15) المؤرخ في 10 نوفمبر 2004.

(2) وكمثال على إجراء تعديل المعطيات في مرحلة الإدخال قيام موظف يعمل في مجال المعالجة الآلية للبيانات بقسم الحاسوب في إحدى البنوك السويسرية الكبرى، بالتلاعب في معطيات المعاملات المالية الخارجية للمصرف، والاستيلاء مع بعض شركائه على مبالغ طائلة، حيث كان يمنع بحكم عمله كمشغل ومراجع للبيانات وصول بعض أوامر تحويل النقود إلى قسم الترميز، ليقوم هو بإدخالها إلى الحاسب،غير انه بدلا من إدخالها مثلما هي عليه فإنه يقوم بضرب القيمة الفعلية لكل أمر في ألف، وقد تمكن بهذه الطريقة من الاستيلاء على 700.000فرنك سويسري، راجع: عبدا لله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، مرجع سابق، ص104.

(3) نائلة عادل محمد فريد قورة، مرجع سابق، ص442.

وبالتالي فإن تعديل المعطيات التي يمكن تطبيق نص المادة(394 مكرر1) عليها يشمل المعطيات التي يتم تعديلها قبل أو أثناء إدخالها، أو تخزينها في نظام المعالجة الآلية للمعطيات، وقبل المرحلة السابقة على إخراجها[1]، وهي ما يمكن أن نطلق عليها مرحلة الإخراج، أي قبل أو أثناء القيام بالأفعال السابقة على صدور الأمر بإخراجها، وتكون العبرة بخروج المعلومات وقد تم تعديلها.

ويتحقق تعديل البرامج عن طريق التلاعب في المدخلات أثناء تنزيل برامج جديدة، أو تعديل البرامج القديمة، أو التلاعب في المخرجات بناء على طلب صاحب النظام، وهذا النوع من التلاعب في البرامج، المتمثل بتعديلها يعد من أخطر أنواع التلاعب، حيث يقوم به جناة متميزون في الجوانب التقنية، ويتم ذلك من خلال وسيلتين[2].

الأولى: تعديل البرامج بعد إعدادها وتجهيزها لتصويب أخطاء تم اكتشافها بها، وهذه المرحلة غالبا ما تتيح للجاني إجراء تعديلات على البرنامج أو البرامج، يكون من شأن تلك التعديلات أن تمكن المجرم من ارتكاب الجريمة التي يخطط لها[3]، وقد يتم ذلك باستخدام البرامج الخبيثة (الفيروسات).

الثانية: أما الوسيلة الأخرى التي يمكن من خلالها تعديل البرنامج بالشكل الذي يرغب الجاني إحداثه فتتمثل في استغلال البرامج المعدة للاستخدام في أوقات الأزمات لتخطي الإجراءات الأمنية الموضوعة[4].

وقد يتحقق فعل المحو، أو التعديل، أو الإدخال عن طريق برامج يتم من خلالها التلاعب في المعطيات، ومن تلك البرامج حصان طروادة (Trojan Horse

---

([1]) راجع: عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، مرجع سابق، ص101.

(2)نائلة عادل محمد فريد قورة، مرجع سابق، ص 247.

([3]) ومن الأمثلة على التلاعب بالبرامج ، قيام شخص يعمل بمركز حاسبات سك حديد بولاية بنسلفانيا من إخفاء 352 عربة شحن كبير، وذلك بقيامة بتعديل برنامج متابعة خط سير عربات الشحن، بحيث يتم توجيه بعض العربات إلى شركة صغيرة للسكك الحديدية بالقرب من شيكاغو، حيث كانت تطلى بلون مغاير وتباع، وكان الجاني بهدف إخفاء الجريمة يقوم بإدخال بيانات في نظام معلومات الحاسوب تفيد بأن هذه العربات إما هالكة أو تحطمت. راجع هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص70.

(4) وكمثال على استغلال البرامج لتخطي الإجراءات الأمنية الموضوعة وتعديل البرنامج : قيام مبرمج بأحد البنوك في الولايات الأمريكية بإجراء تعديلات على أحد البرامج (salami) بحيث يتم إضافة عشرة سنتات إلى كل خدمة تقل قيمتها عن عشرة دولارات، ودولار واحد إلى الخدمة التي تزيد عن هذا المقدار، ثم يتم تحويل المبالغ الزائدة إلى حساب قام الجاني بفتحه تحت اسم وهمي وهو " zzwicke" بحيث يضمن أن يكون هذا الحساب هو الحساب الأخير طبقا للترتيب، واستطاع بذلك أن يحصل على مئات الدولارات، وكانت العملية سوف تستمر لولا أن تم كشفه عندما قام البنك بتكريم أول وآخر عميل، حيث تم اكتشاف أن العميل الأخير ليس له وجود أصلا. راجع: نائلة عادل محمد فريد قورة، مرجع سابق، ص448.

Program)، والذي يعد أحد برامج الفيروسات [1] .كما ظهرت العديد من البرامج التدميرية للبيانات والمعطيات، وكذلك نظام المعلومات في حد ذاته، ومنها برامج ألدودة[2].

وإضافة إلى الفيروسات وبرامج الدودة فقد يتم استخدام القنابل الإلكترونية والتي منها قنابل زمنية وقنابل منطقية [3].

([1]) برنامج حصان طروادة هو برنامج له القدرة على الدخول والاختباء في أي من البرامج الأخرى الموجودة على جهاز الحاسب أيا كان نوعها دون أن يكون صاحب الجهاز على علم بذالك، وتشغيل الفيروس يتم إما عن طريق صاحب الجهاز دون أن يكون على علم بذلك، وذلك في حالة أن يتم ضبط تشغيل الفيروس بأمر أو عملية محددة تستخدم من قبل صاحب الجهاز، والطريقة الأخرى لتشغيل الفيروس تتمثل بقدرة الفيروس على تشغيل نفسه، وقد سمي بهذه التسمية لتشابه آلية عمله مع تلك الفيروسات التي تصيب الكائنات الحية، ومن الأمثلة على التلاعب الذي تسببه الفيروسات، تسبب فيروس غير معروف في إصابة شبكة كاملة من الحاسبات الشخصية لوزارة الدفاع البريطانية في إحدى قواعدها بمدينة بريستول في أوائل عام 2003، وكانت هذه ألشبكة في مجمع عسكري، وكان المسئول عن نظام المشتريات العسكرية، وتسبب في توقف الشبكة عن العمل لمدة ثلاثة أيام كاملة، وأكدت بريطانيا بان الفيروس لم يؤثر على باقي شبكات وزارة الدفاع والشبكات الأخرى في أنحاء بريطانيا. ومثال أخر لاستخدام برامج الفيروسات لإتلاف المعطيات : في ديسمبر 1989 أرسل 20.000شريطا يحتوي على برنامج المعلومات حول السيدا إلى ربع أنحاء العالم، في غلاف يظهر أنه جاء من منظمة الصحة العالمية، وعند استعمال البرنامج لأول مرة يظهر عادة نص الرخصة، يحذر المستخدم ضد الاستعمال بالغش للوجيسيال، ويدعوه إلى دفع ثمنه، وبأنه في حالة عدم دفع الثمن فإن الإجراءات سوف تتخذ ضد الوجسيال، ولقد قام عدة أشخاص باستخدام البرنامج وتبين فيما بعد أن الفيروس خرب كل بطاقيتهم في الحاسوب. كما شهد عام 2004 تزايدا هائلا في التهديدات الأمنية التي تستهدف أجهزة الكمبيوتر التي تستخدم برامج تشغيل ويندوز، وتجاوز عدد الفيروسات المعروفة المائة ألف فيروس = وارتفع عدد الفيروسات الجديدة بنسبة خمسين بالمائة، حسب ما نشر في تقرير دولي لشركة سيمنتيك لمكافحة الفيروسات. راجع: منير محمد الجنبيهى و ممدوح محمد الجنبيهى، امن المعلومات الإلكترونية، دار الفكر الجامعي، الإسكندرية،2005، ص48، وص 60 . وراجع في المثال الثاني: نصرون وردية ، مرجع سابق، ص106. وراجع: جريدة الشرق الأوسط الإلكترونية السعودية الصادرة يوم الخميس 30 ديسمبر 2004 على الرابط .
http://arabic.cnn.com/2006/scitech/4/26/emails.daily/index.html

(2) الديدان (Worms): وهي برامج صغيرة قائمة بذاتها ولا تعتمد على غيرها وقد صممت للقيام بأعمال تدميرية أو بغرض الاستيلاء على بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم لشبكة الإنترنت وإلحاق الضرر بهم أو بالمتصلين بهم، وتتميز بسرعة الانتشار، كما أنه في نفس الوقت يصعب التخلص منها، نظرا لقدرتها الفائقة على التلون والتناسخ والمراوغة، وتعد نوع من أنواع الفيروسات، ولكنها تتميز بسرعة الانتشار والتوالد، بمعنى أن لها القدرة الكبيرة على نسخ برامجها، وتختلف الديدان في طريقة عملها، فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة، بينما يتخصص بعضها بالبريد الإلكتروني بحيث تقوم بإرسال نفسها في رسائل إلى جميع من توجد عناوينهم بالبريد الإلكتروني بالجهاز، وأنواع أخرى تقوم بإرسال رسائل قذرة إلى بعض الموجود عناوينهم في دفتر العناوين الموجود بالجهاز باسم مالك البريد مما يجعل مالك البريد في إحراج مع من أرسلت إليهم الرسائل، وتكمن خطورتها في استقلاليتها وعدم اعتمادها على أي برامج أخرى، مما يعطيها الحرية الكاملة في الانتشار السريع، وأصبح بعضها كابوسا مرعبا لكل ملازم لشبكة الإنترنت ومثال ذلك تلك الدودة التي ظهرت في أكتوبر 2002م واشتهرت باسم (TANATOS) وانتشرت بسرعة كبيرة وخلفت وراءها آثارا تدميرية هائلة، وفي الغالب ما يتم انتشار تلك الديدان عن طريق الرسائل الإلكترونية المفخخة والتي تحمل في العادة عناوين جذابة، راجع: أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص258. منير محمد الجنبيهى، ممدوح محمد الجنبهى، أمن المعلومات الإلكترونية، مرجع سابق، ص68.

(3) تهدف القنبلة المنطقية (logic Bomb)إلى تدمير المعلومات عند حدوث ظرف معين أو لدى تغير أمر ما كشطب اسم أحد الموظفين مثلا، أما القنبلة الزمنية (Time Bomb) فهي تعمل في وقت محدد وفي يوم معين مثل فيروس (shernobel) الذي اكتشف عام 1998، وكمثال للنتائج التدميريه التي تحدثها تلك البرامج ومنها القنابل الإلكترونية حادثة شركة (omega) وتتمثل بقيام مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة (omega) من مدينة (Delaware) ويدعى (timothy Allen Lloyd) 35 عاما بإطلاق قنبلة إلكترونية في عام 1996 (bomb) بعد 20 يوما من فصله من العمل، استطاعت تلك القنبلة أن تلغي كافة التصاميم=

وكما سبقت الإشارة بأن أفعال الإدخال أو التعديل أو المحو تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية، سواء بإضافة معلومات غير صحيحة أو محو أو تعديل معطيات موجودة من قبل، والنشاط الإجرامي في هذه الجريمة إنما يرد على المعطيات أو المعلومات التي تمت معالجتها آليا، والتي تحولت إلى مجرد إشارات أو رموز وليست المعلومات بذاتها، بحيث تقتصر الحماية الجنائية على المعطيات التي توجد داخل النظام وفقا لنص المادة(394 / 1)ع.ج .

كما تمتد الحماية الجنائية إلى المعلومات التي في طريقها إلى المعالجة، أو تلك التي داخلت بعد خروجها، وبالتالي فلا تشمل الحماية الجنائية للمعلومات التي كانت خارج النظام، أو التي كانت مخزنة في أقراص أو أشرطة ممغنطة، ولا يشترط أن تقع تلك الأفعال بطريقة مباشرة بل أنها قد تقع بطريقة غير مباشرة.

وأفعال الاعتداءات العمدية على نظم المعالجة الآلية للمعطيات، والمتمثلة بالإدخال أو المحو أو التعديل وردت في نص المادة (394 / 1) على سبيل الحصر، ويترتب على ذلك بأنه لا يقع تحت طائلة التجريم أي فعل آخر غيرها، حتى لو تضمن اعتداءات على المعطيات داخل النظام، فلا تعد من الأفعال التي ترتكب بها تلك الجريمة فعل التخريب أو السرقة أو استخدامها، لأن تلك الأفعال لا تنطوي لا على تعديل، ولا محو، ولا إدخال(1).

د- النتيجة الإجرامية

لقد سبق توضيح أن النتيجة الإجرامية بالنسبة لجريمة الدخول والبقاء إلى نظام المعالجة الآلية للمعطيات تقتصر على الخطر، ولا يتطلب المشرع لتحقق النتيجة الإجرامية حدوث الضرر، فهي من جرائم الخطر مثلها مثل جريمة التعامل في معطيات غير شرعية والتي سيتم تناولها لاحقا، إلا أن الوضع في هذه الجريمة- التلاعب في

=وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم مستخدمة في (nasa) والبحرية الأمريكية ، ملحقة خسائر بلغت 10 ملايين دولار. راجع: وليد عكوم، ((التحقيق في جرائم الحاسوب)) بحث منشور على موقع منتدى موقع كلية الحقوق-جامعة المنصورة، تم التأكد من أن المقال مازال متاح في الموقع بتاريخ2009/6/7 على الرابط:

http://www.f-law.net/law/showthread.php?t=11336

ولمزيد من التفصيل حول برامج الفيروسات والديدان والقنابل المنطقية راجع عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، مرجع سابق، ص113 وما بعدها، وراجع أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص257 وما بعدها.

(1) راجع: آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص123.

معطيات الحاسوب- يختلف، فهي من الجرائم التي يتطلب لتمامها أن يترتب عليها نتيجة إجرامية تتمثل بالضرر الذي يحدث نتيجةً للسلوك الإجرامي، والمتمثل بتغيير حالة المعطيات عما كانت عليه [1]، وهذه النتيجة- الضرر- هي نفسها النتيجة الإجرامية للجريمة التي يترتب عليها تشديد العقوبة في جريمة الدخول أو البقاء، إلا أنها في الأخيرة غير عمدية، كما أنها تتم بعد عملية دخول أو بقاء غير مصرح بهما، أما في هذه الحالة فإن التغيير أو الإزالة قد تتم نتيجة دخول أو بقاء مصرح أو غير مصرح بهما.

كما أن الجريمة في هذه الحالة تكون دائما عمدية (مثل إزالة العقوبة في صحيفة السوابق العدلية أو تغيير وصفة الدواء للمريض في النظام المعلوماتي في المستشفى)[2].

3- الركن المعنوي لجريمة التلاعب في المعطيات المخزنة في النظام

الركن المعنوي في هذه الجريمة ركن مفترض، فلم تحدد المادة (394 مكرر1) الركن المعنوي بصورة واضحة، إلا أنه من خلال صياغة النص وبالتحديد ذكر المشرع الجزائري لعبارة(كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها) حيث يستدل منها بأن الجريمة جريمة عمدية لا تتحقق إلا إذا ارتكبت عن طريق الغش، ويترتب على ذلك ضرورة توافر القصد الجنائي بعنصريه العلم والإرادة.

فيجب أن يكون المتهم عالماً بأنه يقدم على ارتكاب أفعال تشكل اعتداءات على المعلومات في النظام المعلوماتي، سواء بإدخال معطيات إلى النظام، أو إزالة المعطيات التي يتضمنها، أو تعديل المعطيات .

ويجب أن يعلم بأن المعلومات التي يقوم بالاعتداء عليها هي ملك غيره، وبالتالي فلا تتحقق الجريمة إذا ما قام الشخص بارتكاب أفعال من شانها محو أو تعديل أو إلغاء

([1]) ومن الجرائم المتعلقة بالتلاعب بالمعطيات المخزنة بالنظام والتي تتطلب تحقق نتيجة قيام طفل يبلغ من العمر 14 عاما بالسطو الإلكتروني على حسابات العديد من العملاء من البنوك في عمان بالأردن، بعد أن أخترق السيرفر الرئيس لعدد من البنوك وتحصل على معلومات الحماية مثل (كلمة السر) لعدد منها وأرقام وحسابات عدد من العملاء، وقام بمئات عمليات سحب بمبالغ نقدية صغيرة تقل عن دينار من حسابات العملاء، وتحويلها إلى حسابه، ليسطو بتلك الطريقة على زهاء 12 ألف دينار، موقع إنسان نت، ت.د 2008/8/6 على الرابط:
http://www.ensan.net/news/212/ARTICLE/3520/2008-04-18.html

([2]) نصرون وردية، جرائم الغش في الإعلام الآلي، مرجع سابق، ص104.

معلومات هي في حقيقتها تابعة له، وهو من يحق لـه التصرف بهـا، أو اعتقد أنـه المالـك لتلك المعطيات [1].

ويضـاف إلـى عنصر العلم عنصر الإرادة كعنصر من عناصر الـركن المعنـوي، فلابد أن تتجه إرادة المتهم إلى اقتراف تلك الأفعال، بغض النظر عن الباعث الذي من اجله اتجهت إرادة المتهم لاقتراف ذلك الفعل الذي تتحقق بـه جريمة الاعتداءات علـى المعلومات المخزنة بالنظام المعلوماتي، سواء كانت بدافع الانتقام من صـاحب النظـام أم القائم عليه، أم بغرض تحقيق الكسب المادي، أم غير ذلك من الأغراض.

ويترتب على ضرورة تطلب الإرادة بـأن الجريمـة لا تتحقق كجريمة عمديـة فـي حالـة مـا إذا تـم إزالـة معطيات أو تعديلها أو محوهـا نتيجـة حـادث غيـر مقصـود، حيث يكون الفعل في مثل هذه الحالة خطأ نتيجة للإهمـال أو عدم أخذ الحيطـة والحذر، كمن يوقع شيئا على الجهاز بدون قصد.

فإذا ما توافر القصد الجنـائي بعنصريه العلم والإرادة فلا يهم أن يتجـه ذلك القصـد إلـى الاعتـداء علـى معطيـات جهـات بعينهـا كالمعطيـات المخزنـة فـي الأنظمـة المعلوماتية لجهات هامة، أو معطيات محددة بذاتها كالمعلومـات الخاصـة بـالأمن القومي للدولة، أو المعطيات بشكل عام دون تحديد لأهميتها أو للأنظمة المخزنة عليها، وذلك ما سار عليه التشريع الجزائري وكذلك الفرنسي، بخلاف بعض التشريعات التـي تطلبت قصداً خاصاً كشرط لقيام الركن المعنوي[2].

ويمكن استخلاص القصد الجنائي بعنصريه العلم والإرادة من ظروف وملابسـات الموضوع[3].

ومتى ما تحقق القصد الجنائي العام فإن الجريمة تتحقق، بحيث لا يتطلب المشرع الجزائري في الجريمة وفقا لنص المـادة(394 مكرر1) قصـد جنـائي خـاص، حيث أن لفظ الغش في نص المادة لا يدل على القصد الجنائي الخاص، بقدر مـا يـدل علـى تطلـب

---

(1) احمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 378.

(2) ومن التشريعات التي تتطلب أن تكون المعطيات المستهدفة محددة، التشريع الفدرالي الأمريكي لعام 1986بموجب نص المادة (1030(أ)) والتي تجرم الإتلاف ألعمدي وغير المصرح به لمعلومات حاسب إلي يتبع حكومة الولايات المتحدة الأمريكية أو إدارتها أو حاسب إلي غير تابع للحكومة إلا انه يستخدم من قبلها أو لصالحها، راجع: محمد خليفة، مرجع سابق، ص187.

(3) شيما عبد الغني محمد عطا الله، مرجع سابق، ص152.

ارتكاب الجريمة عمداً، لكون أفعال الإدخال، أو المحو، أو التعديل للمعطيات يقوم بها المختصون في مجال المعلوماتية، ومن ثم لا تكون هناك جريمة إلا إذا ارتكبت بطريق الغش، أي العمد [1].

4- قمع جريمة التلاعب بالبيانات

تكون عقوبة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال، أو عدل بطريق الغش المعطيات التي يتضمنها نظام المعالجة الآلية للمعطيات حسب نص المادة(394 مكرر1) من القانون الجزائري هي: الحبس من ستة أشهر (6) إلى ثلاث(3) سنوات، و غرامة تتراوح من 500.000(خمسمائة الف)إلى 02.000.000(مليوني) دج [2].

يتضح من خلال العقوبة المشار إليها بأن المشرع الجزائري قد شددها في هذه الحالة عن جريمة تعديل أو إلغاء المعطيات المترتبة على جريمة الدخول والبقاء، لكون الجريمة في هذه الحالة ارتكبت عن طريق العمد.

وهو بهذا النهج أي المشرع الجزائري قد حذا حذو المشرع الفرنسي، حيث أن المشرع الفرنسي قد شدد من عقوبة جريمة الاعتداء العمدي على المعطيات المخزنة داخل النظام، عنها في حالة أن تكون نتيجة لجريمة الدخول والبقاء في صورتها المشددة، كما شددها أكثر من خلال التعديلات القانونية المتعاقبة [3].

([1]) كذلك فإن القانون الفرنسي لا يشترط في جريمة التلاعب بمعطيات الحاسوب توافر القصد الجنائي الخاص مكتفيا بالقصد الجنائي العام، بموجب نص المادة (323-3) من قانون العقوبات لعام 2004، وعلى خلاف ذلك فإن بعض التشريعات تتطلب توافر القصد الجنائي الخاص في جريمة التلاعب بالمعطيات المخزنة بنظام المعالجة الآلية للمعطيات ومنها التشريع البرتغالي والفنلندي والتركي كقصد الإضرار بالغير، وقصد تحقيق الربح، ويترتب على ذلك أن بعض المعطيات الهامة والمتعلقة بالجانب العلمي والذي لا يكون الغرض من الاعتداء عليها تحقيق الربح تخرج من نطاق الحماية الجنائية، محمد خليفة، مرجع السابق، ص188.

([2]) المادة (394 مكرر1) من القانون الجزائري رقم (04- 15) المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات.

([3]) شدد قانون العقوبات الفرنسي عقوبة جريمة التلاعب في معطيات الحاسوب نظرا لخطورة الجريمة، فقد كانت العقوبة وفقا لتشريع 1988 هي الحبس من ثلاثة أشهر إلى ثلاث سنوات وبالغرامة من (2000) فرنك إلى خمسمائة ألف فرنك (500.000 ف)، أما قانون 1994 فقد جعل العقوبة تقتصر على الحد الأعلى سوءا الحبس أو الغرامة وجعل عقوبة الحبس ثلاث سنوات إما الغرامة فجعلها خمسة وأربعين ألف يورو (45.000 يورو)، وقد تم تشديد العقوبة في التعديل الثالث للقانون، ففي قانون 2004 أصبحت عقوبة الحبس خمس سنوات والغرامة خمسة وسبعين ألف يورو(75.000يورو)، والعقوبة الأخيرة تضمنها قانون العقوبات لعام 2004 في المادة(323-2).والنص بالفرنسي:

Article 323-2

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)=

المطلب الثالث

جريمة الاعتداء أو التعامل في البيانات خارج النظام

تعتبر جرائم المعطيات من أخطر الجرائم المعلوماتية وأشدها ضررا، وتزيد خطورة تلك الجرائم إذا كانت تلك المعطيات تتعلق بالأمن القومي للدولة، أو بالحياة الخاصة[1].

وتوجد نوعين من الاعتداءات الموجهة ضد المعطيات، منها اعتداءات على المعطيات المخزنة في نظام المعالجة الآلية سبق إيضاحها، واعتداءات على المعطيات خارج النظام.

وقد وفر القانون الجزائري الحماية الجنائية للمعلومات خارج النظام من خلال النص على تجريم التعامل مع تلك المعطيات الناتجة عن إحدى جرائم المعلوماتية المنصوص عليها في القانون، باعتبارها معطيات غير مشروعة، نص القانون على تجريم استخدامها.

كما يوجد نوع أخر من المعطيات يمكن أن ترتكب بها أي من الجرائم المعلوماتية المنصوص عليها في المواد (من 394 مكرر 1- 394مكرر7)ع.ج.

والغاية من تجريم الأفعال التي يمكن أن ترتكب بها إحدى الجرائم المعلوماتية هي غاية وقائية، كون هذه الجرائم خطيرة، ويهدف المشرع من تجريمها إلى منع وقوع الضرر الذي يمكن أن يترتب عليها.

أما التعامل بالمعطيات الناتجة من إحدى الجرائم فإن الهدف من تجريمها هو التخفيف من أثارها قدر الإمكان.

=(Loi nº 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 juin 2004)
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. http://www.legislationline.org/upload/legislations/cd/1b/f05864013134135c992550ab7c98.htm

(1) فتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها تجعل المجتمع يتحول بذلك إلى عالم تصبح فيها أسرارنا وأمورنا الشخصية ومعاملاتنا المالية وحياتنا العقلية والجسمانية مكشوفة. راجع هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مر جع سابق، ص182نقلاعن الفقيه: ارثرميللر، وراجع يونس عرب، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي نقلا عن الفقيه الفرنسي ارثرميللر (Mellor)، منشور على شبكة المعلومات الدولية ، على موقع منديات اليسير للمكتبات وتقنية المعلومات، ، ت.د 2007/6/10.
http://www.alyaseer.net/vb/showthread.php?t=19032

ولم يتناول القانون اليمني تلك الجرائم كغيرها من جرائم المعلوماية، حيث لازالت النصوص التقليدية في قانون العقوبات اليمني هي التي يتم محاولة تطبيقها على تلك الجرائم، مع أنها تثير العديد من الإشكاليات التي قد تحول من تطبيق تلك النصوص.

1- جريمة التعامل في بيانات تصلح لان ترتكب بها جريمة معلوماتية

جريمة التعامل في المعطيات التي تصلح لأن ترتكب بها جرائم المعلوماتية المنصوص عليها في قانون العقوبات الجزائري، تتعلق بالمعطيات التي يتم تجميعها، أو تصميمها، أو نشرها، أو الاتجار فيها، وغير ذلك من الأفعال التي يتم بها ارتكاب إحدى جرائم المعلوماتية، حيث سيتم بيان أركانها تباعا.

أ- الركن الشرعي

نص القانون الجزائري على جريمة التعامل في معطيات يمكن أن ترتكب بها إحدى الجرائم المنصوص عليها في القسم السابع من قانون العقوبات، والمتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث نصت المادة (394مكرر2-1) على أن (يعاقب بالحبس من شهرين (2) إلى ثلاث(3) سنوات، وبغرامة من 1.000.000دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش: بتصميم، أو بحث، أو تجميع، أو توفير، أو نشر، أو الاتجار في معطيات مخزنة، أو معالجة، أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم)[1]، ولقد استمد المشرع الجزائري هذا النص من نص المادة (323- 3 - 1) من القانون الفرنسي[2]. والقانون الفرنسي بدورة استمد النص من الاتفاقية الدولية للإجرام

([1]) المادة (394 مكرر 2) من القانون رقم (04- 15) المؤرخ في 10 نوفمبر 2004. ونص المادة بالفرنسي:
(Art . 394 quater .- (Loi n 04 – 15 du10 Novembre 2004)
Est puni d' un emprisonnement de deux (2) mois à trios (3) ans et d'une amende de 1.000.000 de DA à 5.000.000 de DA, quiconque volontairement et frauduleusement:
1 -conçoit, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique, et par lesquelles les infractions prévues par la présente section peuvent être commises .

(2) Article 323-3-1
(inséré par Loi nº 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004)
Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

المعلوماتي مع استبدال بعض الألفاظ والتي منها على سبيل المثال لفظ الحصول من اجل الاستخدام في الاتفاقية استبدل بدلا عنه في القانون الفرنسي لفظ التجميع[1].

لذا يتضح بأن محل جريمة التعامل في معطيات صالحة لأن ترتكب بها جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، هي المعطيات المخزنة، أو المعالجة، أو المرسلة عن طريق منظومة معلوماتية، بحيث لا يقتصر الأمر على المعطيات

([1]) تضمنت اتفاقية بودابست 2001 لمكافحة الإجرام المعلوماتي في المادة (6) تجريم بعض الأفعال المتعلقة ببعض الأجهزة أو بيانات الولوج، من حيث إساءة استخدامها بغرض ارتكاب إحدى الجرائم المعلوماتية المنصوص عليها بالاتفاقية، وأوجبت على الدول الأطراف في الاتفاقية تبني الإجراءات التشريعية، أو أية إجراءات أخرى بغرض تجريم إنتاج، أو بيع، أو الحصول من أجل الاستخدام، أو استيراد، أو نشر، أو أي أشكال أخرى للوضع تحت التصرف، أي جهاز، يحتوي على برنامج معلوماتي، مصمم أو موافق بشكل أساسي لغرض ارتكاب جرائم المعلوماتية التي تضمنتها الاتفاقية، أو كلمة المرور، أو شفرة الدخول، أو أية بيانات مماثلة تسمح بالولوج إلى كل أو جزء من نظام الحاسوب، أو حيازة أي عنصر من العناصر المشار إليها لارتكاب تلك الجرائم، وخولت المادة لكل طرف أن يشترط في قانونه الداخلي وجود بعض هذه العناصر من أجل تقرير المسؤولية الجنائية، ونوهت المادة بأنه لا يجب أن يفسر نصها نحو تقرير المسؤولية الجنائية حينما تكون تلك الأفعال لا تهدف إلى ارتكاب الجريمة، ونص المادة بالفرنسي:

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu’elles sont commises intentionnellement et sans droit:

a la production, la vente, l’obtention pour utilisation, l’importation, la diffusion ou d’autres formes de mise à disposition:

i d’un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l’une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d’un mot de passe, d’un code d’accès ou de données informatiques similaires permettant d’accéder à tout ou partie d’un système informatique,

dans l’intention qu’ils soient utilisés afin de commettre l’une ou l’autre des infractions visées par les articles 2 à 5; et

b la possession d’un élément visé aux paragraphes a.i ou ii ci-dessus, dans l’intention qu’il soit utilisé afin de commettre l’une ou l’autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu’un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l’obtention pour utilisation, l’importation, la diffusion ou d’autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n’ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d’essai autorisé ou de protection d’un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a. ii du présent article.

راجع: هلالي عبد اللاه أحمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص96، وص97. وراجع شبكة المعلومات الدولية، مرجع سابق، على الرابط :

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

المخزنة في نظام المعالجة الآلية للمعطيات، بل إنه يشمل المعلومات المرسلة عبر منظومة معلوماتية، وهذا ما يجعل هذه الجريمة تختلف عن جريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات أو التلاعب بالمعطيات.

ويهدف المشرع الجزائري من خلال النص السابق إلى حماية المعطيات في حد ذاتها، وعدم حصر هذه الجريمة في المعطيات المعالجة عن طريق نظام معالجة آلية، فوسع المجال، ليشمل مختلف المعطيات مهما كانت حالتها، سواء كانت مخزنة أم مرسلة عن طريق منظومة معلوماتية، أم معالجة آليا، طالما أن الهدف هو استعمالها لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات، وتشمل جرائم الدخول والبقاء، أو الاعتداءات العمدية على المعطيات داخل النظام، أو تخريب النظام كظرف مشدد على جريمة الدخول والبقاء، والتلاعب بالمعطيات المخزنة في نظام المعالجة الآلية للمعطيات[1].

ب- الركن المادي

تضمنت المادة (394مكررر 2) ع ج، العديد من الأفعال التي يمكن أن تستخدم بها المعطيات لارتكاب جريمة معلوماتية، هذه الأفعال تشمل كافة إشكال التعامل الواقعة على معطيات الحاسب الآلي، والتي تسبق استعمال تلك المعطيات في ارتكاب الجريمة، وهي التصميم، أو البحث، أو التجميع ، أو التوفير ، أو النشر، أو الاتجار.

1) التصميم (design)

هو أول عملية في سلسلة التعامل في المعطيات وإخراجها إلى الوجود، بحيث تكون صالحة لارتكاب الجريمة، وهذا العمل يقوم به المختصون كالمبرمجين والمصممين للبرامج، ومثال ذلك تصميم برامج خبيثة تحمل فيروسا، أو برامج اختراق[2].

---

(1) آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص123.

(2) ومثال لتصميم برامج الاختراق، ماقام به طالب نروجي يبلغ من العمر 16 سنه من وضع برنامج صغير قام بتصميمه بمساعدة من والده أطلق عليه أسم(دي سي اس)، وقام بواسطته بكسر الحماية الموضوعة على فلم سينمائي أمريكي، مما ساعد على انتشار الفلم على الشبكة، وتسبب في خسارة الشركة المنتجة للفلم، وقد لجأت شركات الإنتاج السينمائية الأمريكية لرفع دعوى أمام المحاكم الأمريكية لإغلاق اربعة مواقع تتيح تحميل البرنامج مجانا. راجع مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، مرجع سابق، ص64.

فتصميم وإطلاق برامج الكومبيوتر الخبيثة لا تعد أفعالا غير أخلاقيه فحسب، بل إنها تعد أفعالا غير مشروعة (1).

However, some people defend the authors of malicious ومعcode by offering one or more of the following justifications: أن البعض يدافع عن مصممي البرامج التي قد تستخدم لارتكاب جريمة معلوماتية مبررين ذلك بأن تلك البرامج تكشف عن الثغرات الأمنية في الأنظمة المعلوماتية وإمكان إصلاحها، إلا أن تلك المبررات غير مقبولة لأن إطلاق البرامج الخبيثة حتى لو كان بغرض اكتشاف الثغرات الأمنية للنظام في المؤسسة فإن سلبياتها أكثر من إيجابياتها، فهي تكشف أموراً تتعلق بالحياة الخاصة لمالك النظام، أو الأسرار الخاصة بالمؤسسة، بما فيها البيانات الخاصة بالأفراد المخزنة بتلك النظم(2).

كما أنه في الغالب لا يستطيع مصمم البرنامج الذي قام بإطلاقه من السيطرة عليه، مثلما حدث للطالب (موريس) عقب تصميم وإطلاق فيروسه بهدف اكتشاف الثغرات الأمنية في بعض الأنظمة الإلكترونية لبعض الجامعات، وكيف خرج الأمر عن سيطرته(3)، وأصاب آلاف الأجهزة ولعدد من المؤسسات الهامة، بالإضافة إلى أن تصميم وإطلاق البرامج الخبيثة عمل غير مشروع في جميع التشريعات التي وضعت في مجال الإجرام المعلوماتي (4).

---

(1) Copyright 1999, 2002 by Ronald B. Standler Computer Crime http://www.rbs2.com/ccrime.htm

(2) أضحى العدوان على المعلومات الشخصية في مجال المعلوماتية أمراً سهلاً في ظل البرامج المعلوماتية المصممة لهذا الخصوص، فقد أصبحت حياة الفرد وأسرته تكيف تبعا لمصالح معينة لجهات تملك معلومات مخزنة في أنظمتها، وبذلك يصبح الإنسان معاملاً كالأرقام تتحكم في بياناته أجهزة كمبيوتر بحيث تجعلها عرضة للانتهاك مابين لحظة وأخرى، فقد أصبح الحال في ظل التطور التكنولوجي وثورة المعلوماتية أن يكون بمقدور الشخص الذي يتقن أو على الأقل يستطيع التعامل مع التقنية في أن يطلع على معلومات الآخرين منتهكا خصوصياتهم، و زاد الأمر خطورة في مجال الاعتداء على الحياة الخاصة ما توفره شبكة الإنترنت من معلومات عن خصوصيات الأفراد بسبب عدم توفر السرية الكاملة والأمان في الشبكة، فقد أضحت الشركات التي تقوم بتجميع معلومات شخصية تخص الأفراد مثل شركات التامين وغيرها، تعرف تفاصيل الحياة الخاصة للأفراد أكثر مما يعرفه الخطيب عن خطيبته حسب تعبير أحد الكتاب الأمريكيين. راجع محمد عبد الله الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع الشبكة الإنترنت، رسالة ماجستير، كلية الحقوق ،جامعة القاهرة، 2004، ص139.

(3) أراد (روبرت مورس- أمريكي الجنسية) أن يثبت من خلال برنامج قام بتصميمه ضعف نظام الأمن في أجهزة الحواسيب دون أن يسبب أي مشكلة أخرى، حيث كان يضن أن البرنامج واقع تحت سيطرته وبإمكانه التحكم به، إلا أن المفاجأة كانت على خلاف ذلك، حيث خرج البرنامج عن سيطرته، بسبب فا صلة وضعت في غير محلها مما أدى إلى تناسخ البرنامج بشكل تلقائي وعشوائي وإلحاق أضرار متفاوتة بحوالي ستة ألف شركة كانت تمكن الناس من الاستفادة من خدمات الإنترنت. راجع: مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ط1، دار الكتب والوثائق القومية المصرية، القاهرة، 2001، ص30.

(4) Ronald B. Standler, op. cit, http://www.rbs2.com/ccrime.htm.

وإذا كان تجريب بعض البرامج التي تم تصميمها بهدف إيجاد أنظمة حماية أمنية قوية، فإن مثل تلك الأعمال تقتصر على المؤسسات الأمنية المتخصصة، والتي تجرب برامجها على أنظمة تتبعها، أو على برامج خبيثة أطلقها القراصنة، وذلك بهدف توفير الحماية منها.

2) البحث(consideration)

البحث عن وسيلة لارتكاب جريمة لا يعد جريمة، فمن يبحث عن سكين لا يعد مرتكبا لجريمة قتل، ويرجح بأن المشرع الجزائري يقصد بعبارة البحث في نص المادة (394مكرر2): البحث في كيفية تصميم المعطيات وإعدادها، وليس مجرد البحث عن هذه المعطيات ولذلك جاءت عبارة البحث بعد عبارة التصميم مباشرة وان كان النص قد جاء عاما [1].

ونعتقد بأن مصطلح البحث المشار إليه في نص المادة سالفة الذكر يشمل البحث عن كيفية تصميم المعطيات، وإعدادها لترتكب بها جريمة، أو البحث عن معطيات وبرامج يمكن أن ترتكب بها جريمة، لكون البحث عن معطيات جاهزة يكون أسهل من البحث عن كيفية إعدادها، وذلك في ظل العديد من المواقع التي يمكن أن توفر تلك المعطيات .

ويؤكد ذلك سياق نص المادة، الذي يجرم عدد من الأفعال منها فعل البحث، حيث يلاحظ من سياق النص أنه يجرم البحث في معطيات مخزنة، أو معالجة، أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم)

ومن ذلك البحث عن أرقام بطائق الائتمان لكي يتمكن الجاني من استعمالها بطريقة غير مشروعة، أو البحث عن كلمات المرور بهدف الدخول إلى الأنظمة.

كما يمكن القول بأن مصطلح البحث عن الكيفية التي يتم بها أعداد أو تصميم معطيات، أو البحث عن وسيلة أو برنامج لإرتكاب جريمة من الجرائم المعلوماتية المنصوص عليها في القانون الجزائري، يعتبر مرحلة سابقة لمصطلح الحصول من أجل الاستخدام المنصوص عليه في المادة(6) من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي، أو مصطلح التجميع في القانون الجزائري.

([1]) محمد خليفة، مرجع سابق، ص201.

3) التجميع (collage)

ويقصد به القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات، أو جريمة التلاعب في معطيات الحاسوب، أو غيرها من الجرائم المعلوماتية المنصوص عليها.

وهذا النوع من السلوك الإجرامي يفترض بأن صاحبه يحتفظ بمجموعة من المعطيات التي تشكل خطرا يمكن استعمالها في ارتكاب تلك الجرائم، فخطورة الفعل تكمن في التجميع للمعطيات التي يمكن أن ترتكب بها تلك الجرائم، فمن يحوز معطى واحدا لاشك بأنه لا يشكل خطورة بنفس الشكل لمن يحوز عدة معطيات[1].

4) التوفير(الوضع تحت التصرف met a disposition)

يعد فعل التوفير من الأفعال المكونة للركن المادي للجريمة، فمن يقوم بتوفير معطيات يمكن أن ترتكب بها جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للبيانات التي نص عليها القانون الجزائري يعد مقترفا للجريمة، إلا أنه يلاحظ من خلال ترجمة نص المادة (394 -2)ع. ج بأن معنى العبارة في سياق نص المادة تعني "أي أشكال للوضع تحت التصرف " met a disposition " وليس التوفير، وهو ما يتوافق مع اتفاقية بودابست [2].

ويعني التوفير تقديم المعطيات غير المشروعة، وإتاحتها لمن يريدها، ويختلف فعل التوفير عن الفعل السابق له- التجميع- في كون الأخير يقتصر على الشخص الذي يقوم بالتجميع، أما الأول – التوفير – فإنه يتعدى الشخص الذي قام بتوفيرها لإمكانية

([1]) ولم يستخدم القانون الفرنسي الجديد (2004) في المادة(332- 3- 1) مصطلح التجميع بل استخدم مصطلح الحيازة، ولاشك بأن التجميع يقتضي الحيازة، وإن كان يتطلب معطيات لا معطى واحد بعكس لفظ الحيازة التي يمكن أن تشمل معطى واحد وقد تشمل أكثر من معطى، كما أن اتفاقية بودابست لعام 2001 استخدمت مصطلح" الحصول للاستخدام " ولم تستخدم مصطلح التجميع ويميز المصطلح الأول –الحصول للاستخدام – عن المصطلح الثاني –التجميع- في أن الأول يقتضي وجود نية استخدام المعطيات المتحصل عليها، بينما الثاني لا يشترط مثل تلك النية ويشترط تعدد المعطيات.

([2]) ويقابلها نص المادة (323-3-1) من قانون العقوبات الفرنسي الجديد لعام 2004 بالنص على الفعل تحت مصطلح Céder، ونصت على فعل التوفير المادة 6 من اتفاقية بودابست تحت عبارة أي أشكال للوضع تحت التصرف ، لمزيد من التفصيل راجع: محمد خليفة ، مرجع سابق، ص202.

استخدامها من قبل الغير، وجعل المعطيات - التي يمكن أن ترتكب بها جرائم من جرائم المعطيات - في متناول الغير.

ومثال ذلك من يقوم من خلال موقع معين بتوفير أرقام بطائق الائتمان أو الوفاء الخاصة بالغير، أو عناوين بريدهم الالكتروني، أو غير ذلك من المعطيات والبرامج التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية.

وقد يتم من خلال تلك المواقع توفير بيانات، أو صور مخلة بالحياء تم الحصول عليها بطريقة غير مشروعة [1].

ومع أن هذا الفعل – التوفير- عندما يتعلق بصور إباحية تتعلق بالأطفال قد تضمنته اتفاقية بودابست ضمن الجرائم المعلوماتية تحت مسمى تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتي، ضمن جرائم المحتوى، حيث أن مصطلح الإتاحة يعني التوفير[2].

كذلك فقد تضمنتها بعض القوانين العربية الحديثة بنص خاص ضمن نصوص مكافحة جرائم المعلوماتية [3].

أما قانون العقوبات الجزائري فلم يتضمن ضمن النصوص الخاصة بتجريم المساس بأنظمة المعالجة الآلية للمعطيات نصا يجرم توفير الصور أو البيانات ذات العلاقة بالإباحية، أو الاستغلال الجنسي للأطفال، مكتفيا بالنصوص التقليدية لمواجهتها.

5) النشر (Display)

([1]) ومن الأمثلة على تجميع بيانات وصور بطرق غير مشروعة وتوفيرها بهدف إطلاع الغير عليها، قيام عصابة في ايطاليا بأخذ صور شخصية تتضمن مشاهد مخلة بالحياء يتم التقاطها عبر كميرا رقمية صغيرة يصل حجمها إلى حجم علبة الثقاب، وذلك من خلال وضعها في دورات المياه العامة، وغرف الفنادق، وحمامات السونا البخار، وغير ذلك من الأماكن التي يظن فيها الشخص عدم المساس بخصوصياته، بعد ذلك يتم توفير تلك الصور من خلال مواقع بالإنترنت، بمقابل 15دولار للكتلوج . راجع مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ص185

([2]) تضمنت المادة الفقرة (1) بند (ب) من المادة (9) من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي (بودابست 2001) النص على تجريم تقديم أو إتاحة مادة إباحية طفوليه عبر نظام معلوماتي. راجع هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست، مرجع سابق، ص119.

([3]) ومن تلك القوانين الخاصة بمكافحة جرائم المعلوماتية التي تضمنت فعل التوفير أو ما يدل عليه لمواد إباحية، أو مخلة بالآداب العامة، القانون الإماراتي، من خلال نص المادة(12) والتي تضمنت تجريم عدد من الأفعال التي تؤدي إلى المساس بالآداب العامة ومنها العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه المساس بالآداب العامة، وتشديد العقوبة في حال أن تكون تلك الأفعال موجه إلى الأحداث. كذلك فقد تضمن القانون السعودي الخاص بمكافحة جرائم المعلوماتية في الفقرة (1) من المادة(6)، النص على تجريم عدد من الأفعال ذات العلاقة بالمساس بالنظام العام، أو القيم الدينية ، أو الآداب العامة، أو الحياة الخاصة، عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.

يعد فعل النشر من الأفعال التي نصت عليها المادة (394 مكرر2)، وهذا الفعل يعد من عناصر الركن المادي للتعامل مع المعطيات التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية، كما يعد أحد عناصر الركن المادي للجريمة في صورتها الثانية، أي عندما تكون المعطيات ناتجة عن إحدى جرائم المعلوماتية[1].

و يقصد بفعل النشر: نقل المعطيات محل الجريمة، وتمكين الآخرين من الاطلاع عليها، بحيث يشمل كل نشاط من شأنه نقل البيانات إلى الآخرين [2].

ويقصد به في هذه الجريمة: التوزيع الايجابي للمادة المجرمة[3]، أي التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية.

ويعد فعل النشر من أخطر أفعال الركن المادي في جريمة استعمال المعطيات غير الشرعية لارتكاب إحدى جرائم المعطيات، إذ أن هذا الفعل كفيل بأن ينقل المعطيات إلى عدد كبير من الأشخاص، مما يجعل احتمال استعمال تلك المعطيات في ارتكاب الجرائم بنسبة كبيرة مقارنة بالأفعال الأخرى.

ويختلف فعل النشر عن التوفير في أن التوفير يتطلب من الشخص البحث عن المعطيات التي يمكن من خلالها ارتكاب إحدى جرائم المعلوماتية، وتحميلها وتوفيرها للآخرين، بخلاف النشر الذي يفترض فيه أن المعلومات متوافرة لدى الشخص أو الموقع الذي يتبعه، لاكنه لا يكتفي بتوفيرها للآخرين إنما يقوم بنشرها بإحدى وسائل النشر.

6) الاتجار (Commercialization)

يشمل فعل الاتجار بالمعطيات كل أنواع التعاملات التي يمكن أن تنصب على المعطيات التي تكون محلا لأن ترتكب بها إحدى الجرائم المنصوص عليها في المواد من (394مكرر إلى 394مكررر7) من القسم السابع من ق.ع. ج والمتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات.

---

(1) ويقابلها المادة السادسة من اتفاقية بودابست حيث نصت على فعل النشر ، بخلاف ق.ع.ف والذي لم يتضمن فعل النشر، مما يجعل المتبادر إلى الذهن بأن المشرع الجزائري قد عمل على التوفيق بين الاتفاقية الدولية للإجرام المعلوماتي – بودابست- والقانون الفرنسي.

(2) إبراهيم حامد طنطاوي، أحكام التجريم والعقاب في قانون تنظيم الاتصالات المصري رقم(10) لسنة 2003، ص15.

(3) هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص124.

ولم تتضمن اتفاقية بودابست فعل الاتجار، لا كنها تضمنت فعلي البيع والاستيراد[1] وهما يقابلان مصطلح الاتجار المنصوص عليه في القانون الجزائري، وعدد من القوانين[2].

وبالتالي فيكون الاتجار المجرم، هو الاتجار بالمعطيات أو الأجهزة التي يمكن أن ترتكب بها إحدى جرائم المعلوماتية، ومن ذلك الاتجار بأي جهاز يحتوي برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض ارتكاب إحدى جرائم المعلوماتية، كما يشمل الإتجار ببيانات المرور، أو شفرة الدخول، أو أي بيانات مماثلة تسمح بالولوج إلى كل أو جزء من نظام الحاسب بغرض ارتكاب جريمة من الجرائم المعلوماتية [3].

ويختلف فعل الاتجار عن فعل التوفير في أن الاتجار يقدم وفق مقابل معين، أما الثاني التوفير فيمكن أن يقدم بدون مقابل، والمشرع الجزائري حين نص على الفعلين أراد أن يجرم كل أنواع التعاملات سواء كانت بمقابل أم بدون مقابل .

ج- الركن المعنوي

جريمة التعامل في معطيات غير شرعية جريمة عمدية في صورتيها، وفقا لنص المادة(394مكرر2) حيث ورد في نص المادة لفظ"عمدا وعن طريق الغش "والعمد في هذه الجريمة يتطلب توافر القصد الجنائي العام والقصد الجنائي الخاص .

([1]) لم تتضمن اتفاقية بودابست 2001، وفقا لنص المادة (6) فقرة(1) بند(أ) مصطلح الاتجار، وإنما تضمنت مصطلح "البيع والاستيراد"، أما القانون الفرنسي فقد تضمن مصطلح الاستيراد، ويكون المشرع الجزائري بنصه على الاتجار قد شمل البيع والاستيراد وغيرها من التعاملات التي يتصور وقوعها على المعطيات، كما أن المشرع الفرنسي قد نص على مصطلحي التوفير والعرض أو العرض تحت التصرف، وما يميز هذين المصطلحين عن الاتجار هو أن الاتجار يكون بمقابل، بينما التوفير أو العرض قد يكون بمقابل أو بدون مقابل، وقد نص المشرع الجزائري على الفعلين معا. راجع: محمد خليفة، مرجع سابق، ص204.

([2]) تعاقب عدد من التشريعات على الاتجار بالمعطيات أو كلمات السر لاستخدامها بأغراض غير مشروعة، ومن ذلك التشريع الأمريكي الذي ينص على عقاب كل شخص يقوم بقصد الغش بالاتجار بكلمات المرور، واستطاع أو مكن الغير من الدخول إلى جهاز الكمبيوتر إذا كان ذلك يؤثر على التجارة بين الولايات المتحدة الأمريكية وبينها وبين الخارج، وإذا كان جهاز الكمبيوتر يستخدم من قبل حكومة الولايات المتحدة الأمريكية، ولا تكتفي تشريعات أخرى بتجريم الاتجار بالمعطيات، بل إنها تجرم مجرد حيازة المعطيات لاستخدامها في ارتكاب جرائم تتصل بالمعلوماتية ومن ذلك التشريع الكندي . لمزيد من التفصيل راجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص137وص138.

([3]) راجع هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص97.

حيث تعتبر جريمة التعامل مع معطيات غير شرعية، يمكن أن يتم بها ارتكاب جريمة معلوماتية من الجرائم التي نص عليها القانون، جريمة عمدية يتطلب لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة .

فلابد أن يعلم الجاني بكل العناصر التي تدخل في بناء الجريمة، فلابد أن يعلم أنه يتعامل مع معطيات غير مشروعة، يمكن أن يتم بواسطتها ارتكاب أي من جرائم المعطيات، ومنها جريمة الدخول أو البقاء غير المشروع، أو جريمة التلاعب بمعطيات الحاسوب بتعديلها أو محوها، وبناء على ذلك فإن العلم بأن المعطيات عادية ولا علاقة لها بالجريمة ينفي القصد الجنائي.

كما يتطلب لقيام الجريمة أن تتوافر الإرادة، والإرادة في هذه الجريمة تنصب على السلوك الإجرامي، كونها من الجرائم الشكلية التي لا تتطلب لتمامها تحقق نتيجة معينة، وبالتالي فان الإرادة تقتصر على السلوك المتمثل بأحد الأفعال المشار إليها من تصميم، أو بحث، أو تجميع، أو توفير، أو نشر، أو اتجار، بنية ارتكاب جريمة من الجرائم المعلوماتية المنصوص عليها في القسم السابع من قانون العقوبات الجزائري.

ولايكفي لقيام جريمة التعامل في معطيات غير شرعية تصلح لأن ترتكب بها جريمة معطيات توافر القصد الجنائي العام، بل لابد أن يتوافر القصد الجنائي الخاص إلى جانب القصد العام، أي اتجاه العلم والإرادة إلى وقائع معينة لا تدخل في تكوين الجريمة.

ويتحقق القصد الجنائي الخاص في التعامل بالمعطيات التي تصلح لأن ترتكب بها جريمة، ويتحقق ذلك بالتمهيد والإعداد لاستعمالها في ارتكاب الجريمة، وهي مسألة نفسية محضة، أما استعمال المعطيات في ارتكاب جريمة فليست ركنا في هذه الجريمة، فقد لا يقوم احد باستعمال هذه المعطيات ومع ذلك تقوم الجريمة [1]

([1]) محمد خليفة ، مرجع سابق ، ص213

واشتراط العمد في الجريمة، يتطلب توافر القصد الجنائي العام والخاص، وبالتالي ينتفي القصد ولا تقوم الجريمة حينما ترتكب تلك الأفعال بهدف استخدام المعطيات أو الأجهزة من أجل الاختبار المصرح به، أو لحماية جهاز الحاسب[1].

د- العقوبة

تضمنت المادة (394 مكرر 2) النص على عقاب التعامل مع المعطيات الغير شرعية سواء التي يمكن أن ترتكب بها الجرائم المرتبطة بالمعطيات أو المتحصلة منها بالحبس من شهرين(2) إلى ثلاث(3) سنوات وبغرامة من 1.000.000(مليون) دج إلى 5.000.000 (خمسة مليون) دج .

إضافة إلى عقوبة تكميلية أو أكثر من العقوبات المنصوص عليها في الاحكام المشتركة لجرائم المعلوماتية.

2- جريمة التعامل في البيانات المتحصله من جريمة معلوماتية

الصورة الثانية من صور جريمة التعامل في معطيات غير شرعية، تتمثل بالتعامل في المعطيات المتحصلة من إحدى جرائم المعلوماتية، فالمعطيات في هذه الجريمة هي نتاج إحدى جرائم المعلوماتية، وبالتالي فإنها معطيات غير مشروعة.

والفارق بين هذه الصورة والصورة التي سبقتها، هي أن عدم شرعية المعطيات في الصورة السابقة في كونها يمكن أن ترتكب بها جرائم المعلوماتية مثل تصميم برامج اختراق، أو نشر كتب لتعليم الطرق التي ترتكب بها تلك الجرائم، أما في هذه الصورة فتاتي عدم شرعيتها في كونها نتاج إحدى جرائم المعلوماتية، فالتعامل في الصور الإباحية التي تم الحصول عليها من خلال جريمة الدخول والبقاء سواء بحيازتها، أو بنشرها أو غير ذلك من الأفعال التي سيتم الإشارة إليها أثناء تناول الركن المادي للجريمة، تعد جريمة قائمة بذاتها .

([1]) اشترطت المادة (6) من اتفاقية بودابست للعقاب على الوسائل الصالحة لارتكاب جريمة من الجرائم المعلوماتية التي تضمنتها الاتفاقية في المواد من 2- 5 أن يكون التعامل بتلك الوسائل أو المعطيات بنية ارتكاب جريمة، بينما تضمنت الفقرة الثانية من المادة ذاتها عدم فرض المسؤولية الجنائية حينما يكون إنتاج أو بيع أو الحصول من أجل الاستخدام أو الاستيراد أو النشر أو الأشكال الأخرى للوضع تحت التصرف، ليس بهدف ارتكاب جريمة، وفقا لمواد الاتفاقية، في حالة حماية الحاسب أو اختبار النظام. راجع: هلالي عبد أللاه أحمد، مرجع سابق، ص 152.

أ- الركن الشرعي

يتمثل الركن الشرعي للجريمة بنص المادة (394 مكرر2) فقرة (2) حيث نصت على: (يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000 دج إلى 5000.000 د ج كل من يقوم عمداً وعن طريق الغش بما يأتي : حيازة، أو إفشاء، أو نشر، أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم) [1].

يلاحظ من خلال هذا النص بأن المشرع الجزائري قد تطرق إلى تجريم أفعال الحيازة، أو النشر، أو الإفشاء، أو استعمال المعطيات المتحصل عليها من إحدى الجرائم المعلوماتية المنصوص عليها في المواد (من 394 مكرر1 إلى 394 مكرر7)، وذلك لكون التعامل مع تلك المعطيات يعد جريمة بحق الفاعل الذي تحصل عليها، لأنها غير مشروعة، والتعامل معها بحيازتها، أو نشرها ، أو استعمالها لاشك بأنه سيوسع من دائرة الأشخاص الذين يمكن أن يتعاملوا مع تلك المعطيات ويستخدمونها استخداما غير شرعي لأي غرض كان سواء بغرض التحريض على الفسق، أو الفجور، أو الإرهاب، أو أي جريمة كانت.

فالمعطيات المتحصل عليها من إحدى جرائم المعلوماتية هي بلا شك معطيات غير مشروعة، وقد تتمثل في كشف أسرار الناس وأدق خصوصياتهم، وقد تكون من الأسرار الخاصة بالدولة.

فقد يقوم بعض المجرمين في المجال المعلوماتي بمعرفة كلمة المرور لأنظمة معلوماتية تتبع جهات أو شركات، ومن ثم يقومون بعرضها للبيع بهدف الكسب المالي أو الانتقام من تلك الشركات أو الجهات، كما أن بعض المجرمين قد يقومون بعرض تبادل

([1]) راجع :ألفقرة (2) من المادة (394 مكرر 2)من ق. ع.ج (رقم 04 – 15)المؤرخ في 10 نوفمبر 2004.
ونص المادة بالفرنسي:

Art . 394 quater .- (Loi n 04 – 15 du10 Novembre 2004)) (Est puni d' un emprisonnement de deux (2) mois à trois (3) ans et d'une amende de 1.000.000 de DA à 5:000:000 de DA, quiconque volontairement et frauduleusement:
2- détient, révèle, divulgue, ou fait un usage quelconque des données obtenues par l' une des infractions prévues par la présente section) .

كلمات السر التي يحصلون عليها وتخص الغير، ويقومون بعرضها على بعضهم البعض.

ب- الركن المادي

يقوم الركن المادي لهذه الجر يمه على العديد من الأفعال وهي: الحيازة، أو النشر، أو الإفشاء، أو استعمال المعطيات المتحصل عليها من إحدى الجرائم المعلوماتية المنصوص عليها في المواد (من 394 مكرر1 إلى 394مكرر7) :

1) الحيازة:possession

يقصد بالحيازة الاستئثار بالشيء على سبيل الملك والاختصاص دون حاجة إلى الاستيلاء المادي عليه [1].

ويتحقق فعل الحيازة بسيطرة الجاني على المعطيات المتحصلة من جريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، أو جريمة التلاعب بمعطيات الحاسوب وغيرها من الجرائم المنصوص عليها في قانون العقوبات الجزائري وتتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

ولا يتحقق فعل الحيازة إلا بسيطرة الحائز على المعطيات واستغلالها، ويكفي للقول بوجود السيطرة على المعطيات إذا لم توجد عقبات واقعية تحول بين الشخص والتمتع بتلك المعطيات [2].

وتجريم حيازة المعطيات المتحصلة من جريمة الدخول والبقاء، أو غيرها من الجرائم المعلوماتية المنصوص عليها، إنما هي بسبب كونها ناتجة عن جريمة معلوماتية، أي عمل غير مشروع، وبالتالي فإن مجرد حيازة تلك المعطيات يعد عمل غير مشروع، حيث وهي في حد ذاتها معطيات غير مشروع الحصول عليها، أو حيازتها.

---

(1) إبراهيم حامد طنطاوي، مرجع سابق، ص198.

(2) محمد زكي أبو عامر، قانون العقوبات الخاص، ط5، دار الجامعة الجديدة، الإسكندرية، 2005، ص762، مشار إليه لدى محمد خليفة، مرجع سابق، ص206.

ومثال ذلك من يقوم بالدخول الغير مصرح به على أنظمة الغير، أو بريدهم الإلكتروني، ويسيطر على البيانات الخاصة بهم، أي يحوزها، ومن ثم قد يستخدمها في التهديد أو الابتزاز(1).

2) الإفشاء: disclosure

يعد الفعل الثاني الذي يقوم عليه السلوك الإجرامي في الركن المادي لهذه الجريمة محل الدراسة هو فعل الإفشاء لتلك المعطيات المتحصلة من إحدى جرائم المعلوماتية، لما يمثله ذلك الفعل من خطورة تجعل تلك المعطيات في متناول أكثر من شخص.

ولا يشترط لتحقق فعل الإفشاء أن يكون الشخص الذي قام بإفشاء المعطيات هو الشخص المؤتمن عليها وإنما يتحقق الفعل من أي شخص كان.

كما لا يشترط في تحقق فعل الإفشاء إعطاء قدر معين من المعلومات، بحيث يتحقق الفعل وتقوم الجريمة ولو كانت المعلومات التي تم إفشاؤها قليلة (2).

3) النشر :diffusion

يعد فعل النشر من عناصر الركن المادي الذي استوجب القانون تحققه، سواء في التعامل مع المعطيات التي يمكن أن ترتكب بها جريمة، أم في هذه الصورة المتعلقة بالمعطيات المتحصلة من إحدى جرائم المعطيات، نظرا لخطورة هذا الفعل الذي بتحققه يتمكن العديد من الأشخاص من الاطلاع على المعطيات، ومن ثم تطويعها لارتكاب الجرائم.

ومن قبيل فعل النشر ما يقوم به (الكراكرز)(3) من اختراق لمواقع خصومهم والحصول على كلمة المرور، ومن ثم القيام بنشرها على الجميع إضرارا بأصحابها(4).

---

(1) ومثال لفعل الحيازة غير المشروع الناتج عن أحدى جرائم المعلوماتية، قيام شاب في المملكة العربية السعودية بحيازة صور فتاة تحصل عليها نتيجة قيامة لاختراق بريدها الإلكتروني، ومن ثم القيام بتهديدها بنشر تلك الصور، وقد تم ضبطه وصدر حكم بسجنه وفقا لنظام مكافحة جرائم المعلوماتية السعودي. صحيفة الوطن السعودية، الأحد 2008-12-21،

http://www.almotamar.net/news/65627.htm

(2) إبراهيم حامد طنطاوي، مرجع سايق، ص153.

(3) يختلف الهاكر (Hhacker) عن الكراكر (Cracker) في أن الصنف الأول يكون غرضه الاختراق والوصول إلى أقوى أنظمة الحماية الأمنية واختراقها، إلا أنه غير مؤذ، فلا يقوم بالإتلاف أو تخريب الأنظمة والمعطيات التي تحتويها، حيث يظل الهدف الدائم لهذا الهاكر هي محاولة الدخول والاختراق فقط، بخلاف الكراكر الذي يحمل نوايا إجرامية للقيام بكل ماهو سيء وشرير من إتلاف وتخريب للأنظمة والمعطيات. راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص240.

(4) ومن قبيل ذلك فقد أُلقي القبض على فتى يبلغ من العمر 18 عاما ضمن حملة دولية كبيرة، حيث قبض عليه شمال نيوزيلاند باسم" أكيل" بدلاً من اسمه الحقيقي، وتقول الشرطة: إنه مسؤول عن عصابة دولية قامت=

كما يقوم فعل النشر في حالة نشر معلومات مخزنة بأنظمة معلوماتية، تم الحصول عليها، كنتيجة لارتكاب إحدى جرائم المعلوماتية ومنها جريمة الدخول إلى النظام [1].

ولا يشترط لتحقق فعل النشر أن يتكرر لأكثر من مرة، بل إن النشر ولو لمرة واحدة يجعل الفعل قائما.

كما أنه لا يشترط أن يتم النشر بوسيلة معينة، سواء عن طريق الأقراص، أو الانترنت، أو حتى الكتابة.

4) الاستعمال : application

إذا كان الإفشاء والنشر فعلين من الأفعال التي يقوم عليها الركن المادي نظرا للخطورة التي بتحققهما تصبح المعطيات في متناول الغير، فإن فعل الاستعمال يعد أشد خطورة من سابقيه، لكونه ينتقل من مجرد احتمال ارتكاب الجريمة بتحقق الأفعال السابقة إلى اقترافها فعلا إذا تحقق فعل الاستعمال.

ويتحقق الفعل إذا ما تم اقترافه ولو لمرة واحدة فقط، أي أنه لا يشترط تكراره حتى تقوم الجريمة.

ومن قبيل ذلك استخدام كلمة المرور، أو أرقام بطائق الائتمان التي تم الحصول عليها نتيجة ارتكاب جريمة معلوماتية، ومن ثم القيام باستعمالها [2].

=باختراق كومبيوترات في أنحاء العالم، من خلال تحميل برامج خاصة فيها تقوم بإرسال معلومات شخصية حساسة من تلك الكومبيوترات إلى أجهزة أفراد العصابة، بما فيها أرقام بطاقات ائتمان وكلمات سر وبيانات حسابات مصرفية. منشوره على موقع مجلة التقنية والاتصالات،ت.د 2009/11/14 على الرابط:
http://www.mnafe-it.com/index.php?id=155

(1) وكمثال لتحقق فعل نشر معطيات كأحد الأفعال المجرمة الناتجة عن جريمة الدخول إلى أنظمة معلوماتية، قيام صبي بريطاني في السادسة عشر من عمره من اختراق أحد أجهزة الحاسب الآلي الرئيسية في وزارة الدفاع الأمريكية، ومن ثم قيامة بنشر معلومات عبر شبكة الإنترنت عن أبحاث الصواريخ البالستية، وتصميم الطائرات، وقوائم الأجور، وملفات العاملين، والبريد الإلكتروني. راجع: مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، مرجع سابق، ص63.

(2) تمكن شاب استرالي يبلغ من العمر 16سنة من الدخول إلى أحد المواقع البولندية على شبكة الإنترنت، وقام بتحميل البرامج التي تستخدمها البنوك لكي يتوصل إلى الترتيب العشوائي لترقيم بطائق الائتمان، وبعد أن توصل إلى أرقام صحيحة لبطائق الائتمان، استعملها في شراء أجهزة كمبيوتر تبلغ قيمتها 37 الف$ استرالي، وبعد اكتشاف أمرة حكمت عليه محكمة بريسبيان بوضعه تحت المراقبة لمدة عامين ومائة ساعة من العمل الجماعي. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، مرجع سابق، ص68.

ج- الركن المعنوي

الركن المعنوي في جرائم الإعلام الآلي مفترض، وجريمة التعامل مع المعطيات المتحصلة من إحدى جرائم المعلوماتية المنصوص عليها في قانون العقوبات الجزائري، جريمة عمدية يشترط لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة.

فيشترط لقيام جريمة التعامل بالمعطيات المتحصلة من إحدى الجرائم المنصوص عليها في المواد (من 394 مكرر1 إلى 394 مكرر7) ع.ج، أن يكون الجاني عالما بأن تعامله مع تلك المعطيات سيرتب أضرارا إضافية إلى تلك الجريمة التي تم الحصول على المعطيات منها.

كما يجب أن يعلم بالصفة غير المشروعة للمعطيات التي يتعامل بها، وبالتالي فإن القصد ينتفي في حالة عدم توافر العلم بأن المعطيات غير مشروعة.

إضافة إلى عنصر العلم فلابد من توافر عنصر الإرادة حتى يتحقق القصد الجنائي العام في جريمة التعامل بمعطيات ناتجة عن جريمة.

فلا بد لمن يقوم بنشر، أو إفشاء، أو استعمال تلك المعطيات غير الشرعية أن يقدم على تلك الأفعال بإرادة حرة، ومدركة لما يقوم به.

ولا يتطلب في هذه الصورة قصداً جنائياً خاصاً، لكون التعامل مع المعطيات الناتجة عن جريمة هو في حد ذاته جريمة وعملا غير مشروع.

وما ورد في نص المادة (394 مكرر 2) من إضافة عبارة "عن طريق الغش" إلى عبارة "عمدا " في هذه الجريمة والاقتصار على عبارة "عن طريق الغش" فقط لبقية الجرائم الخاصة بالمساس بأنظمة المعالجة الآلية لمعطيات، لا يستدل منه على ضرورة تطلب القصد الجنائي الخاص في هذه الجريمة كشرط لاقترافها، بقدر ما يدل على تأكيد العمدية ليس إلا.

وكان الأولى أن يكتف بلفظ عن "طريق الغش"، كونه يعبر عن العمدية طالما أنه تم استخدام اللفظ في جرائم الدخول والبقاء والتلاعب بالمعطيات[1].

(1) محمد خليفة، مرجع سابق، ص217.

د- العقوبة

عقوبة هذه جريمة التعامل بالمعطيات المتحصلة من إحدى جرائم المعلوماتية المنصوص عليها، هي نفس العقوبة المشار إليها في جريمة التعامل مع معطيات يمكن أن ترتكب بها جريمة معلوماتية، حيث تضمن ق.ع.ج على عقوبة الصورتين في نص قانوني واحد[1].

حيث تكون العقوبة هي الحبس من شهرين إلى ثلاث سنوات، وغرامة من 1000.000 دج إلى 5000.000 دج.

إضافة إلى العقوبات التكميلية التي تمت الإشارة إليها أثناء تناول الأحكام المشتركة لجرائم المعلوماتية.

---

(1) راجع المادة (394 مكرر2) من القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004 المتمم لقانون العقوبات الجزائري.

المطلب الرابع

جريمة الاعتداءات العمدية على سير نظم المعالجة الآلية للمعطيات

يقصد بجريمة الاعتداءات العمدية على نظام المعالجة الآلية للبيانات كافة الأفعال التي من شأنها أن تؤدي إلى إعاقة، أو إفساد النظام، وتتسبب في بطئ عمله أو إيقافه عن العمل[1].

وتعد الاعتداءات العمدية على سير نظم المعالجة الآلية للمعطيات من أهم جرائم المعلوماتية، نظرا لما تحدثه من آثار خطيرة على أمن المجتمع واقتصاده، لأن توقف أنظمة معنية عن العمل قد يتسبب في كارثة بيئة أو صحية، مثل الاعتداءات التي يتم توجيهها إلى الأنظمة الالكترونية التي تعمل بواسطتها مؤسسات الصرف الصحي أو الكهرباء، أو المؤسسات ذات الطابع الإنتاجي.

1- الركن الشرعي

لم يورد المشرع الجزائري نصا يجرم الاعتداءات العمدية على سير نظام المعالجة الآلية للمعطيات ضمن نصوص المساس بأنظمة المعالجة الآلية للمعطيات، مكتفيا بنصوص وردت في مواد أخرى، بعضها يجرم الاعتداءات العمدية على المعطيات الموجودة داخل النظام، والبعض الآخر يجرمها كظرف مشدد على جريمة الدخول والبقاء.

حيث نصت المادة (394 مكرر1)، على أنه **(يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من 5000.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها)**[2].

كما نصت الفقرة الثالثة من المادة(394 مكرر) على: (وإذا ترتب على الأفعال المذكورة- الدخول والبقاء- تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى150.000 دج)[3].

([1]) هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص92.

([2]) المادة (394 مكرر 1): من القانون الجزائري رقم (04 – 15) المؤرخ في 10 نوفمبر 2004 .

([3]) راجع: الفقرة(3) من المادة (394 مكرر) من نفس القانون.

ومن خلال النصين السابقين، يتضح بأن الأول يقتصر على تجريم إدخال معطيات إلى النظام، أو تعديل أو إزالة المعطيات التي يتضمنها بطريقة عمدية.

أما النص الثاني فيجرم الاعتداء على النظام كظرف مشدد على جريمة الدخول والبقاء، وليس لهما علاقة بتجريم الاعتداء العمدي على سير النظام.

ولعل تفسير الاكتفاء بتجريم الاعتداء على المعطيات كمبرر للاعتداء على النظام في نظر المشرع الجزائري وفقا لنص المادة(394 مكرر1)، يرجع إلى أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، وقد تؤدي إلى إعاقة النظام وإفساده [1]، حيث أن حماية المعطيات تعد حماية غير مباشرة للنظام لا كن ذلك غير كاف[2].

حيث يلاحظ على ذلك التفسير بأنه يكون سليما حينما يكون ذلك الاعتداء الذي وقع على المعطيات وسيلة وليس غاية، فإن الفعل حينئذ يشكل جريمة الاعتداء العمدي على النظام، بينما لا يكون كذلك في حالة ما إذا كان الاعتداء على المعطيات يشكل غاية - مثلما هو في النص السابق- ، وليس وسيلة حيث أن المعطيات هي المستهدفة وليس النظام.

هذا بالإضافة إلى أن المشرع الجزائري قد نص على محو أو تعديل المعطيات، أو الاعتداء غير العمدي على سير النظام كظرفين مشددين لجريمة الدخول والبقاء في نص المادة (394 مكرر)، وبالتالي فان الاعتداءات العمدية على سير النظام تفلت من العقاب، بينما جريمة الاعتداء العمدي على المعطيات تعاقب وفقا لنص المادة(394مكرر1)،

والواقع فإن التمييز بين إتلاف المعلومات وبين إعاقة النظام عن أداء عمله ومعاملتهما كسلوكين منفصلين أمر تتطلبه الاعتبارات العملية، حيث أنه يمكن أن يكون هناك إتلاف للمعلومات والبرامج دون أن يترتب على ذلك إعاقة النظام، كما في بعض الحالات التي يتم فيها إتلاف بعض الملفات التي يتضمنها النظام دون أن يؤثر ذلك على وظيفته، وبخلاف ذلك فيمكن أن يحدث إعاقة لنظام الحاسب الآلي باستخدام أي وسيلة منطقية دون أن يترتب على ذلك إتلاف للمعلومات والبرامج التي يتضمنهما [3].

---

(1) محمد خليفة، مرجع سابق، ص175.
(2) آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص114.
(3) نائلة عادل محمد فريد قورة، مرجع سابق، ص2004.

وبالتالي فإن على المشرع الجزائري أن يتدارك ذلك القصور بالنص على تجريم الاعتداء على النظام كجريمة عمدية، مثلما فعل المشرع الفرنسي[1] .

حيث جرم القانون الفرنسي الاعتداءات العمدية على سير نظام المعالجة الآلية للبيانات مستقلة عن جريمة الاعتداءات على البيانات التي يتضمنها النظام ، وبذلك يكون قد توسع في قاعدة حماية سير نظم المعلوماتية من حيث الدخول إليها، أو إلغاء المعطيات التي تحتويها، أو إعاقتها أو إفسادها، نظرا لخطورة تلك الأفعال على الأنظمة في حد ذاتها، سواء تعلق الأمر بنظم عامة أو مفتوحة للجمهور، وخاصة فيما يتعلق بنظم العمل الداخلية وقطاعات المعلومات الحساسة، هذا بالإضافة إلى أن هناك حالات يمكن أن يأتي فيها الاعتداء على النظم المعلوماتية من الخارج، دون المرور إلى النظام نفسه، مثل بث البرامج التي من شانها أن تؤثر على سير النظام المعلوماتي، أو على الشبكات التي تغذيه[2].

كذلك فقد جرمت بعض القوانين العربية المستحدثة الاعتداء العمدي على النظم المعلوماتية [3].

([1]) تضمنت المادة (323- 2)ع. ف 1994 (عقوبة إعاقة أو الإخلال بسير نظام المعالجة الآلية للمعطيات بالحبس مده لا تزيد عن خمس سنوات والغرامة التي لا تزيد عن 300000 فرنك، ويقابلها نص المادة (462- 3)من نصوص القانون رقم 19 لعام 1988 حيث تعاقب على تعطيل أو إفساد تشغيل نظام المعالجة الآلية للبيانات بالحبس من ثلاثة أشهر إلى ثلاث سنوات وغرامه من 10.000 إلى 100.000فرنك، كما نص عليها قانون العقوبات الفرنسي المعدل لعام 2004 في المادة(323-2) وجعل عقوبتها الحبس مدة خمس سنوات والغرامة 75000يورو. ونص المادة 323 -2 كما وردت بالقانون الفرنسي

Article 323-2

(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 juin 2004)

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

([2]) أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص354.

(3) تضمن قانون مكافحة جرائم تقنية المعلومات الإماراتي في المادة (5) والمادة (6) على تجريم إعاقة أو تعطيل الوصول إلى الخدمة، أو الدخول إلى الأجهزة بأية وسيلة كانت عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، وكذلك تجريم إدخال عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه إيقافها عن العمل أو تعطيلها. وتضمن نظام مكافحة الجرائم المعلوماتية السعودي في المادة(5) النص على تجريم الاعتداء على الشبكة المعلوماتية بإيقافها عن العمل، أو تعطيلها، وكذلك إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت. كما تضمن قانون العقوبات القطري رقم (2004/11) في نص المادة(374) تجريم إتلاف، أو تخريب عمداً وحدات الإدخال، أو الإخراج، أو شاشة حاسب آلي مملوك للغير، أو الآلات، أو الأدوات المكونة له، وكذلك تعطيل شيء مما سبق أو جعله غير صالح للاستعمال.

2- الركن المادي

يقوم الركن المادي لجريمة الاعتداءات العمدية على سير نظام المعالجة الآلية للمعطيات على فعل الإعاقة ، أو الإفساد.

ويقصد بالإعاقة منع النظام من العمل بصفة كلية، أو بصفة جزئية، ويكون ذلك بفعل يتسبب في تباطؤ عمل النظام وإرباكه، ويؤدي إلى تغيير في حالة النظام على نحو يعيبه بشكل مؤقت.

وتتمثل أساليب الإعاقة في تعديل البرنامج في نظام المعالجة، أو عمل برنامج احتيالي، أو من خلال إغراق موقع site على الشبكة بالرسائل الإلكترونية مما يؤدي إلى شله[1].

أما التعطيل أو الإفساد فهو: جعل النظام غير قابل للاستعمال، والتعطيل يفترض وجود عمل إيجابي، سواء كانت الوسيلة المستخدمة مادية أم معنوية إذا استهدفت الكيانات المنطقية للنظام، مثل البرامج والمعطيات بإتباع العديد من التقنيات منها:

- إدخال برنامج فيروسي.
- شغل النظام بمعلومات ومعطيات تفوق سعته.

ويستوي بعد ذلك أن يشمل التعطيل جميع مستعملي النظام أم بعضهم، كما يستوي أن يكون التعطيل دائماً أم مؤقتاً .

ويكون تعطيل النظام ناتجاً عن نشاط إيجابي، مثل إغراق النظام بالرسائل، أو إرسال فيروسات تدميرية لإتلاف النظام[2]، والأمثلة على ذلك كثيرة[3] .

(1) احمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص223 .

(2) يمكن للفيروسات المعلوماتية أن تصيب منظومة التحويل الإلكتروني للأموال والودائع وتعطي أوامر خاطئة لسحب رؤوس أموال مما يتسبب في انهيار بنوك ومؤسسات مالية، كما يمكن لها أن تظهر تزويرا لنتائج ما يظهره نظام معلوماتي من مسابقات أو نتائج انتخابية وغيره، كما يمكن لها – أي الفيروسات- من التسلل إلى أنظمة التحكم في الصواريخ والمركبات الفضائية وجعلها تخالف خط سيرها وقد تنفجر في الهواء، كما قد تصيب الفيروسات أنظمة التحكم في شبكات الدفاع فتؤثر على العمليات الحربية وتشل حركتها، وقد تصيب أنظمة المجمعات الكيميائية والمفاعلات النووية وتسبب خللا ينتج عنه تسرب كيميائي أو إشعاعي، وفيما بين الخطر الواقع والمحتمل للفيروسات فإن بعض الخبراء يقول بأن الأسوأ لم يأت بعد وأننا لم نرى شيئاً . راجع هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص158.

(3) ومن القضايا التي ضبطت في مجال إتلاف النظام باستخدام برامج الفيروسات، في بريطانيا اعتقلت وحدة مكافحة جريمة الحاسوب بشرطة المدينة مع المكتب الوطني الفنلندي للتحقيق، وقسم شرطة (Pori) ثلاثة أعضاء مشتبه بهم من عصابة فيروس (Moop) ، وكانت الشرطة البريطانية قد تنبهت لوجود جزء من عصابة دولية من مجرمي الإنترنت في أراضيها، واعتقلت ثلاثة بريطانيين أعمارهم 19 سنة، و28 سنة، و63 سنة، جميعهم من اسكتلندا لارتباطهم بمؤامرة لإصابة أنظمة الحاسبات، ويتضمن ذلك دودة(Worm 32)وحصان طروادة، الذي أُرسل عن طريق البريد الإلكتروني في ملف يحتوي الدليل على ملف تآمر توني بلير وجورج بوش لرفع أسعار النفط ، موقع صحيفة العالم الرقمي ،الجزيرة ،ع 174، الأحد 12رجب 1427 ،الموفق 8/6/ 2006، على الرابط:
http://www.al-jazirah.com/digimag/06082006/wr7.htm

ويتم القيام بأخطر الهجمات التي تستهدف تعطيل النظام وإيقافه عن العمل من خلال ضخ سيل من المعلومات والرسائل عن طريق البريد الإلكتروني، تؤدي إلى عدم قدرة النظام المستهدف على التعامل معها، أو تجعله مشغولا وغير قادر عن التعامل مع الطلبات الصحيحة.

ولم تقتصر الاعتداءات المعلوماتية على النظم، بل شاعت أيضا الهجمات المتعمدة لتعطيل مواقع الإنترنت(1).

ويلاحظ على القانون الجزائري بأنه لم يتضمن في نصوصه تجريم الاعتداء على مواقع الإنترنت وغيرها من جرائم الإنترنت، ولعله بذلك قد اكتفى بتجريم الاعتداء على النظام المعلوماتي، باعتبار أن الموقع الإلكتروني يعمل من خلال نظام معلوماتي، مع أن عدد من القوانين المستحثة ومنها قوانين بعض الدول العربية قد عرفت نظام المعالجة الآلية للمعطيات بتعريف يختلف عن تعريف المواقع الإلكترونية، فنظام المعالجة الآلية للمعطيات هو عبارة عن مجموعة من البرامج والأدوات المعدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية، أو غير ذلك، بخلاف الموقع الإلكتروني الذي هو: عبارة عن مكان لإتاحة المعلومات على شبكة الإنترنت(2).

وفي كل الحالات يجب أن تكون الإعاقة دون وجه حق، فالأنشطة العادية المتضمنة في تصميم الشبكات، أو تطبيقات شائعة للتشغيل، أو لممارسات التجارة، أو إذا كان الأمر يتعلق باختبار نظام الحاسب أو حماية أمن نظام معلوماتي، والمصرح بها من قبل المالك أو القائم بالتشغيل، أو عند إعادة تنظيم نظام التشغيل، عندما يتطلب تشغيل النظام كيانا منطقيا جديد، كما في حالة تشغيل كيانات منطقية للولوج عبر الإنترنت مما

---

(1) ومن الأمثلة على الإعاقة الكلية أو الجزئية للنظام المعلوماتي، ما حدث مؤخر من إعاقة موقع جريدة الوطن السعودية وتعطيله عن العمل لمدة ثلاث ساعات ابتداء من الساعة السادسة من صباح يوم السبت الموافق 2009/11/7، واستمرت حتى التاسعة وثلاث وأربعون دقيقة من نفس اليوم، حيث قام المخترقين للنظام بتعريض الموقع لحركة فيضانيه كبيرة، عبر دخول عشرات الآلاف دفعة واحده، أدت إلى إحداث الخلل فيه، وحسب إفادة رئيس تحرير الصحيفة أن الاختراق الذي تعرض له موقع الصحيفة الالكتروني قادته منظمة تعمل من الجزائر ولها فروع في مختلف أنحاء العالم منها أمريكا وإيران ودول أخرى. وقد ورد الخبر في عدد من المواقع الإخبارية منها موقع مأرب برس، الأحد2009/11/8، على الرابط:
http://marebpress.net/news_details.php?sid=19910

(2) راجع الفقرتان (3، 8) من المادة (1) من نظام مكافحة جرائم تقنية المعلومات الإماراتي رقم (2) لسنة 2006، وراجع الفقرتان (2، 9) من المادة(1) من نظام مكافحة الجرائم المعلوماتية السعودي.

يثبط البرامج المماثلة التي أدخلت من قبل، كل تلك الأنشطة تعتبر شرعية وبالتالي لا يتم العقاب عليها، ولو نتج عنها إعاقة جسيمة[1].

ويختلف فعل إفساد النظام عن التعطيل، في أن الإفساد لا يتسبب في توقف النظام كليا أو جزئيا، وإنما يتسبب في إفساده، أي جعله غير صالح للاستعمال السليم بأن يعطي نتائج مخالفة للنتائج المتعين الحصول عليها، بخلاف التعطيل حيث ينتج عنه توقف النظام عن العمل، كما أن فعل الإفساد يقترب من فعل التعييب المنصوص عليه كظرف مشدد في جريمة الدخول والبقاء في الأثر الذي يترتب على كل منهما في نظام المعالجة الآلية للمعطيات، إلا أن فعل الإفساد يتطلب أن يكون الجاني قد قصد ارتكاب الفعل، بخلاف التعييب، حيث لا يشترط أن يكون ارتكابه بطريقة عمدية، ولذلك فإنه في حالة الإضراب عن العمل الذي قد يسبب في شل حركة الحاسب الآلي، لا يعد جريمة ولا ينطبق عليها نص المادة (323 -2) من القانون الفرنسي لعام 1994، وهي نفس المادة في ق.ع.ف 2004 التي تعاقب على إعاقة سير نظام الحاسب الآلي، كون ذلك يتعلق بالحريات والتعبير عن الرأي، طالما لم يتوافر القصد الجنائي، ولم يكن ذلك مجرما إلا إذا كان مقصودا من الإضراب إعاقة سير عمل الحاسب الآلي.

ويثار التساؤل فيما إذا كان المشرع الفرنسي يشترط لوقوع الجريمة أن يقع إتلاف جزئي أم أنه يتطلب أن يكون الإتلاف كليا .

وفعلا، فإن مجرد عرقلة العمل بالنظام يؤدي إلى قيام الجريمة، ومرد ذلك أن هذه الحالة هي نفسها كحالة التعديل والمحو أو الإلغاء للمعلومات المنصوص عليها في المادة(394مكرر1)ع.ج، بل نها قد تأخذ شكلاً أوسع من الأشكال المتبعة في قرصنة المعلومات، ولذلك فإن النص ينطبق على كل إضرار بسير العمل، سواء نجم عنه إتلاف للمعطيات، أو اقتصر على مجرد المحاولة، فالمشرع في هذه الجريمة يعاقب عليها بعقوبة الجريمة ذاتها .

3- الركن المعنوي

تعد هذه الجريمة من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي العام المبني على العلم والإرادة لاقترافها.

([1]) هلالي عبدا للاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست 2001، مرجع سابق، ص92.

إذ يجب أن يكون الجاني عالما بأنه يرتكب جريمة اعتداء على نظام للمعالجة الآلية للبيانات، وأن من شان فعله إتلاف النظام، أو تعطيله، أو الانتقاص من قيمته بشكل يجعله غير صالح للاستعمال(1).

كما يجب أن يعلم أن النظام الذي يقوم بالاعتداء عليه سواء بالإعاقة أم الإفساد أو التعطيل هو نظام مملوك للغير.

ويتعين إضافة إلى عنصر العلم أن تتجه إرادة الجاني إلى التخريب، والإتلاف، أو التعطيل، أو إعدام الصلاحية لنظام المعالجة الآلية للمعطيات، فإذ انتفت تلك الإرادة فلا توجد جريمة، لانتفاء الركن المعنوي، وعلى سبيل المثال، العامل الذي يكسر اسطوانات عليها معطيات وبيانات أثناء قيامه بالتنظيف، فإنه لا يسأل عن جريمة إتلاف، وكذلك الضيف الذي انزلق عليه كوب ماء أو أي مشروب آخر قدم إليه من مضيفه وتسبب في إتلاف نظام يتبع مضيفه أو موجود لديه، فإنه لا يسأل عن جريمة إتلاف للنظام(2).

وقد تطلبت بعض التشريعات إضافة إلى تحقق القصد العام، توافر القصد الجنائي الخاص، المتمثل بإحداث الضرر لمالك النظام أو المستفيد منه(3)، كون الفاعل يعلم مسبقا بأن فعل الإعاقة أو الإفساد للنظام المعلوماتي لاشك سيترتب عليه إحداث ضرر للغير.

إلا أن تشريعات أخرى أكتفت بتوافر القصد الجنائي العام لتحقق جريمة إعاقة أو إفساد النظام ومنها التشريع الفرنسي، بعد أن كان يتطلب توافر القصد الجنائي الخاص في قانون 1988، وذلك بسبب النقد الذي وجه لتطلب القصد الخاص والمتمثل بأن تطلب توافر القصد الخاص سوف يؤدي إلى استبعاد الحالات التي لاتتجه نية الفاعل إلى تحقيق الربح.

4- العقوبات

طالما أن المشرع الجزائري لم ينص على تجريم الاعتداء على سير نظام المعالجة الآلية للمعطيات بنص مستقل، فإن العقوبة التي يمكن تطبيقها في هذه الحالة هي عقوبة

---

(1)محمد أمين الشوابكة: الجريمة المعلوماتية، رسالة ماجستير،جامعة عمان العربية للدراسات العليا، ط1، دار الثقافة،عمان، الأردن، 2004، ص221.

(2) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 323.

(3) ومن تلك التشريعات التي تطلبت وجوب توافر القصد الخاص بجانب القصد العام في جريمة إعاقة أنظمة الحاسبات الآلية، القانون البرتغالي حيث يتطلب أن تتجه نية المتهم إلى الإضرار بالغير ، أو إلى تحقيق ربح غير مشروع له أو للغير، وكذلك القانون الفنلندي حيث يتطلب أن تتجه نية الفاعل إلى الإضرار بالغير، وكذلك التركي الذي يشترط نية إيذاء الغير أو الحصول على ربح مادي. رجع نائلة عادل محمد فريد قورة، مرجع سابق، ص225.

الاعتداءات العمدية على المعطيات التي يتضمنها النظام، لان الاعتداء عليها يؤثر على سير النظام مع أن المعطيات هي المستهدفة من الجريمة وليس النظام.

بالإضافة إلى العقوبة المنصوص عليها في حالة وجود ظرف مشدد لجريمة الدخول والبقاء، مع أنها في هذه الحالة غير عمدية، ،وذلك بهدف حماية النظام من أي اعتداء عليه.

وبسبب قصور تلك النصوص وحتى يتدارك المشرع الجزائري عدم وجود نص بصورة صريحة يتضمن تجريم إعاقة أو إفساد نظام المعالجة الآلية للمعطيات عندما تكون الجريمة عمدية وتستهدف النظام بالدرجة الأولى، وإزالة للالتباس فيجب عليه أن يضمن التعديل القادم للقانون النص على تجريم إعاقة أو تخريب نظام المعالجة الآلية للمعطيات[1].

5- جريمة الإتلاف المعلوماتي في القانون اليمني

لم يتناول قانون العقوبات اليمني رقم 12 لعام 1994 بنصوص صريحة ما يتعلق بجريمة الإتلاف الواقعة على نظم المعلوماتية، كما لم تتناول الدراسات الفقهية في الجمهورية اليمنية رأي الفقه بصدد نصوص ق.ع المتعلقة بجريمة الإتلاف الواردة في الباب الثاني - المواد من 137،و138 الجرائم ذات الخطر العام – وذلك بهدف الخروج بمعرفة هل بالإمكان تطبيق تلك النصوص على إتلاف نظم المعلوماتية أم لا؟

لذا سوف يتم بحث مدى إمكانية تطبيق النصوص التقليدية على جريمة الإتلاف المعلوماتية، على ضوء الآراء الفقهية وموقف ق.ج.ع.ي إزاء الخلاف في هذه المسألة.

أ- إتلاف المكونات المادية

إن إتلاف النظام المعلوماتي بمكوناته المادية مثل أجهزة الحاسب بشاشات العرض والكابلات ولوحة المفاتيح والأقراص الممغنطة، وغير ذلك من المكونات ذات

([1])تضمن المادة (323-2) من قانون العقوبات الفرنسي لعام 1994 على عقوبة جريمة تعطيل أو إفساد نظام تشغيل نظام المعالجة الآلية للبيانات بالحبس لمدة ثلاث سنوات والغرامة مبلغ 300.000 فرنك. بينما تم تشديد العقوبة وفقا للقانون الفرنسي الجديد 2004 وفقا لنص المادة 323 -2 والتي شددت من عقوبة الحبس من ثلاث =سنوات إلى خمس سنوات والغرامة بدلا من 300.000 فرنك وفقا لقانون 94 إلى 75.000يورو وفقا لقانون 2004. بخصوص ق.ع.ف 1994 راجع: جميل عبد الباقي الصغير، الانترنت والقانون الجنائي –الأحكام الموضوعية لجرائم الانترنت، دار النهضة العربية، القاهرة،2002 ، ص62. وبخصوص النص الأخير ع.ف 2004. راجع شبكة المعلومات الدولية، مرجع سابق، على الرابط:
http://www.legislationline.org/upload/legislations/cd/1b/f05864013134135c992550ab7c98.htm

الطبيعة المادية، سواء كانت تحوي برامج أو كانت خالية من البرامج، فإن مثل هذه المسألة لا تثير أية مشكلة في تطبيق نصوص قانون العقوبات التقليدية، لكون هذه المكونات تدخل في نطاق الأموال المادية بمعناها التقليدي[1].

ولا محل للخلاف في هذه المسألة حول تطبيق المواد(137 و138)[2]، من ق.ج.ع.ي إذا توافرت الشروط الأخرى التي تطلبتها تلك النصوص .

ب- إتلاف المكونات اللامادية

الموضوع الذي يثير الإشكال هو مدى انطباق النصوص التقليدية على المكونات المنطقية والمعنوية للنظام المعلوماتي، وبهذا الخصوص فقد وجد خلاف فقهي بين مؤيد ومعارض :

أما أصحاب الاتجاه المؤيد فيروا بأنه لا يوجد ما يحول وقوع جريمة الإتلاف على برامج وبيانات النظام المعلوماتي، وانطباق النصوص التقليدية عليها[3]. ومبرراتهم هي :

1) أن الخلاف في هذه المسألة هي في وصف المال بأنه مادي، وليس في الطبيعة المالية ذاتها للجانب غير المادي من برامج وبيانات النظام المعلوماتي، وذلك لكون المعلومات سواء تمثلت ببرامج أو قواعد بيانات ونظم تشغيل، فإن الطبيعة المالية لها تمثل الجانب الأكبر من قيمة النظام ككل، وجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من أجله، وذلك ما يجعله يفقد قيمته الحقيقية، ولذلك فإن إتلاف البيانات والبرامج لا يتطلب أن يكون مصاحبا لإتلاف مادة الوعاء التي تحوي ذلك البرنامج أو تلك البيانات، وإنما يكفي أن يتم الإتلاف باستخدام نفس الوسيلة المنطقية وهي المعلومات.

---

(1) عفيفي كامل عفيفي، مرجع سابق، ص186.

(2) تنص المادة (137) بأن: (يعاقب بالحبس مدة لا تزيد عن عشر سنوات كل من أشعل حريقا أو أحدث انفجارا في مال ثابت أو منقول، ولو كان مملوكا له متى كان من شأن ذلك تعريض حياة الناس أو أموالهم للخطر، وتكون العقوبة الحبس مدة لا تقل عن ثلاث سنوات إذا حصل الحريق أو الانفجار في مبنى مسكون أو محل آهل بجماعة من الناس أو في أحد المباني أو المنشئات ذات النفع العام أو المعدة للمصالح العامة). وتنص مادة(138) بأن (يعاقب بالحبس مدة لا تزيد على عشر سنوات:
- من عرض للخطر عمدا وسيلة من وسائل النقل البرية أو البحرية أو الجوية أو عطل سيرها بأية طريقة.
- من عطل بأية طريقة وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العامة.

(3) هدي قشقوش، جرائم الحاسب الآلي في التشريع المقارن، مرجع سابق، ص75 ، احمد خليفة الملط، مرجع سابق، ص636، عفيفي كامل عفيفي، مرجع سابق، ص 186، هشام رستم، مرجع سابق، ص313 حيث لا يروا مانعا من تطبيق نص ألماده (361) من قانون العقوبات المصري على جريمة الإتلاف على برامج وبيانات النظام المعلوماتي.

2) أن نصوص المواد التي وردت في قوانين العقوبات التقليدية قد وردت عامة، ولا تفرق بين الأموال المادية والأموال ذات الطبيعة المعنوية.

3) أن بيانات وبرامج النظم المعلوماتية تعتبر من قبيل الأموال، بالنظر إلى ما تمثله من قيمة اقتصادية ، وبالنظر إلى ما ترد عليها من تصرفات قانونية، تجعلها قابلة للاستحواذ عليها وتملكها، وما يترتب على ذلك من ضرورة توفير الحماية الجنائية لها .

4) لمواكبة التطور التكنولوجي الذي يلحق بالأشياء فيغير من طبيعتها، فتظهر أشياء جديدة لم تكن موجودة من قبل، فلابد من مواجهتها بنصوص تتعامل معها وتحميها، وبالنظر إلى جريمة الإتلاف التقليدية وصلاحيتها، لأن تطبق على إتلاف بيانات وبرامج النظام المعلوماتي، فلا يوجد ما يحول دون ذلك، وأن ذلك يتماشى مع ما يقضي به التطور التكنولوجي[1] .

والنتيجة تظهر عدم انطباق النصوص التقليدية على إتلاف بيانات وبرامج النظام المعلوماتي، وهي وجهة نظر أصحاب الاتجاه الثاني، وذلك لانتفاء الصفة المادية لبرامج وبيانات النظام، باعتبار أن تلك النصوص يقتصر تطبيقها على الأشياء ذات الطبيعة المادية لأسباب أهمها:

1) انتفاء صفة المال عن البرامج والبيانات في النظام المعلوماتي، وعدم قابليتها للملكية باعتبار أن حق الملكية لا ينصب إلا على الأشياء المادية ذات القيمة الاقتصادية [2].

2) باعتبار أن محو البرامج والبيانات يتم في الأساس عن طريق التدخل في وظائف النظام المعلوماتي، لا على الدعامات المادية التي يحتوي البرامج والبيانات[3].

3) لو كانت النصوص التقليدية التي تقرر الحماية الجنائية لجريمة الإتلاف المعلوماتية -برامج وبيانات النظم المعلوماتية- كافية، لما تصدت الدول التي لها السبق في التطور التكنولوجي لتلك الجريمة بنصوص أو قوانين متخصصة لمواجهتها، وفرضت الحماية الجنائية لها، فالحقيقة التي يشهد لها التاريخ أن الكثير من التحولات في الفكر القانوني كانت نتيجة لتحولات تقنية وصناعية، كما أن للقانون دائما رد فعل في مواجهة كل تقدم

([1]) عفيفي كامل عفيفي، مرجع سابق، 189.
([2]) جميل عبد لباقي الصغير، مرجع سابق، ص 159.
([3]) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص159.

علمي[1]، ومن باب أولى كان على الدول العربية مسايرة تلك الدول، إن لم يكن في مجال التطور، ففي مجال التشريع على الأقل فيما يخص مواجهة الجرائم الناتجة عن التطور التكنولوجي.

ونستخلص من هذه الدراسة عدم انطباق النصوص التقليدية على جريمة الإتلاف المعلوماتي، وذلك لاختلاف طرق ارتكابها، واستنباط الأدلة وتكييفها، للمبررات السابق ذكرها إضافة إلى:

1) أن القانون اليمني في نص المادة (137) قد اقتصر في بيانه للوسائل التي يتم بواسطتها الإتلاف على وسائل مادية، يؤدي تنفيذ الجريمة بواسطتها إلى إتلاف الأشياء المادية، وإذا حدث إتلاف لبرامج وبيانات نظام معلوماتي وفقا لنص المادة(137) فلا بد أن يسبق ذلك تدمير الوعاء الذي يتضمن ذلك البرنامج وتلك البيانات، كمايلاحظ بأن نص هذه المادة قد اقتصر على وسيلتي التفجير والحريق لاقتراف جرائم الإتلاف، وبالتالي فيمكن أن تنطبق على إتلاف المال المعلوماتي المادي، مثل الأجهزة وتوابعها إذا استخدمت بواسطة هذين الفعلين ليس إلا.

كما يلاحظ على النص المشار إليه بأنه قد تطلب عدة شروط لتحقق جريمة الإتلاف وهي :

- شرط يتعلق بجريمة الإتلاف في ظرفها المشدد، وهو أن يكون من شأن تلك الأفعال – التفجير والحريق – تعريض حياة الناس للخطر، وفي هذه الحالة تكون العقوبة الحبس مدة لا تزيد عن عشر سنوات.
- شروط تتعلق بالجريمة –الإتلاف- في صورتها المخففة، وهي إما أن تستهدف تلك الأفعال محلاً مسكوناً أو محلاً أهلاً بالسكان، أو في أحد المباني والمنشآت ذات النفع العام أو المعدة للمصالح ألعامة.

2- أن المادة (138) وإن تضمنت في الفقرة الثانية إتلاف أو تدمير وسائل الاتصال بأية طريقه، إنما كانت تهدف بحسب النص إلى الوسائل المادية من كابلات وأجهزة، وبالتالي تخرج من تطبيق النص إتلاف برامج وبيانات نظم المعلوماتية، إذ تنص المادة (138) على الحبس مده لا تزيد عن عشر سنوات لكل:

---

(1) محمد حسن قاسم، مراحل التفاوض في عقد الملكية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، بدون ذكر العام، ص59.

- من عرض للخطر وسيلة من وسائل النقل البرية أو البحرية أو الجوية أو عطل سيرها بأي طريقة كانت.

- من عطل بأية طريقة وسيلة من وسائل الاتصال السلكية أو أللاسلكية المخصصة للمنفعة العامة).

وبالتالي فإذا لم يكن من شأن تلك الأفعال تعريض حياة الناس للخطر ،أو إذا لم يتم ارتكاب تلك الأفعال في مكان مسكون أو محل أهل بالسكان، أو لم يتم استهداف مبان ومنشات ذات نفع عام، أو معدة للمصلحة العامة فلا تتحقق جريمة الإتلاف وفق نص المادة 137، وهذه الشروط إذا توافرت في جرائم الإتلاف للكيانات المادية المعلوماتية بأن يتم استهداف الكيانات المادية للحاسوب وتوابعه، وتوافرت باقي الشروط التي تم ذكرها فلا يوجد مانع من تطبيق نص المادة 137، وإذا كان تطبيق النص المشار إليه يبدو في غاية الصعوبة في مجال الأموال المعلوماتية المادية لكونه لا يشمل الأموال الداخلة في نطاق الملكية الخاصة، أو إذا كان الخطر يقتصر على أماكن ليست مسكونة أو محلات آهلة بالسكان، فانه ومن باب أولى لا تتوافر الحماية الجنائية لجريمة الإتلاف للأموال المعلوماتية المنطقية [1]..

وحتى لا يترك مثل أولئك المجرمين الخطرين في تماديهم على قيم الأفراد ومبادئ المجتمع ونظم الدول، فيجب على المشرع اليمني أن يسرع بتعديل قانون العقوبات وإضافة مواد تتعلق بعقاب الإجرام المعلوماتي، ومنها جرائم الإتلاف واقترح مضاعفة العقوبة في حالة ما إذا كان الإتلاف يستهدف جرائم ذات طابع معلوماتي في الجانب المنطقي، سواء تم الدخول إلى تلك الأنظمة من مستخدمي النظم أو من غيرهم، وسواء كان الدخول من شبكة داخلية أو خارجية أو عن بعد .

([1]) تضمنت الجرائم المتعلقة بالإتلاف المادي عدد من المواد التي أتت مجتمعة في ق.ج.ع.ي رقم 12 لسنة 1994 ومنها المواد (من 136 إلى 147) التي نصت على الإتلاف الناتج عن الجرائم ذات الخطر العام والتي تتسبب في إتلاف المنشات العامة والخاصة، إضافة إلى المواد التي أتت متفرقة بالقانون والتي منها المادة(128) وتضمنت عقوبة إتلاف أسرار الدفاع لمصلحة دولة معينة، والمادة(143) تضمنت عقوبة إتلاف الطرق العامة، والمادة(150) وتضمنت إتلاف مواد إنتاج أو مواد أوليه للإنتاج، والمادة(175) وتضمنت عقوبة إتلاف الأختام الموضوعة على محل أو أوراق، والمادة (176) وتضمنت عقوبة إتلاف أوراق أو دفاتر أو سجلات متعلقة بمصالح الدولة أو المصالح الحكومية أو الشركات، والمادة(184) وتضمنت عقوبة إتلاف الصك أو المحرر الذي كتب بهدف الاستناد إليه، والمادة(255) وتضمنت عقوبة إتلاف الرسائل البريدية، والمادة(261) وتضمنت عقوبة إتلاف المساجد أو دور العبادة المرخص لها، والمادة(319) وتضمنت عقوبة إتلاف أوراق محجوزة قضائيا، والمادة(321) وتضمنت عقوبة إتلاف العقارات أو المنقولات والنباتات غير المملوكة لمن قام بإتلافها، والمادة(323) وتضمنت عقوبة من أتلف أو أزال علامة أو محيط لضبط المساحات.

الباب الثاني

القواعد الإجرائية للجرائم المعلوماتية

الباب الثاني

القواعد الإجرائية للجرائم المعلوماتية

بعد أن تم تناول أهم الجرائم المعلوماتية في الباب الأول، وبيان مدى تناسب النصوص القانونية التقليدية لكي تنطبق عليها أو على البعض منها، والخروج بضرورة إعادة النظر في النصوص التقليدية في قوانين العقوبات حتى يُستَطَاع من خلالها مواجهة تلك الجرائم، أو استحداث قوانين خاصة بمواجهة الإجرام المعلوماتي، وتلافي أي قصور في القوانين أو النصوص المستحثة، إلا أن ذلك غير كافٍ في ظل ما تتسم به أفعال مجرمي المعلوماتية من قدرة على إخفاء الأدلة التي يمكن أن تعين الجهات المختصة في الوصول إليهم ومعاقبتهم، إذ يبدو جلياً صعوبة السيطرة على البيانات والأرقام التي يتم تداولها عبر الإنترنت[1] وبالتالي صعوبة تطبيق جميع قواعد القانون الإجرائي التقليدي عليها، لأنها وضعت من أجل عالم مادي، في حين أن ما يتم في الشبكة وأنظمة المعلوماتية من معاملات، أو اعتداءات على النظم، أو البيانات الموجودة فيها، أو المنقولة من نظام إلى آخر، إنما يتم في فضاء افتراضي.

وقد ظهرت بظهور المعلوماتية العديد من المشكلات الإجرائية منها مشكلات تتعلق بالتحري والاستدلال وأخرى تتعلق بالتحقيق، وثالثة تتعلق بالاختصاص القضائي، وتعد إحدى المشكلات الأكثر صعوبة في مجال الإجرام المعلوماتي، مشكلة التلاعب في الأدلة الإلكترونية وإخفائها، ومدى حجية تلك الأدلة في الإثبات، ومن ثم صعوبة تحديد فاعل الجريمة، وإزاء ذلك فقد أصبح من الضرورة بمكان إعادة النظر في قوانين الإجراءات الجنائية، حتى تفي بمواجهة تلك الجرائم إجرائيا، فتلك الجرائم من واقع طبيعتها ووسائل

([1]) وكمثال لصعوبة السيطرة على البيانات التي يتم تداولها عبر الإنترنت ومن ثم صعوبة إقامة الدليل عليها، قضية ما يسمى بالسر الكبير للرئيس الفرنسي السابق فرنسوا ميتران، حيث قام كل من الطبيب الخاص بالرئيس الفرنسي MITTERRAND والصحفي M. G0NODبنشر كتاب عام 1996 يتضمن الكشف عن مرض الرئيس، والذي كان سببا في وفاته، وبعد أن قام أقاربه برفع دعوى قضائية لإيقاف نشر الكتاب وسحب النسخ التي وزعت، حيث رأت أن الكتاب يتضمن إفشاء لأسرار أحد أفرادها البارزين، وبموجب ذلك فقد أصدر القضاء المستعجل بتاريخ 18 يناير 1996حكما يقضي بحظر نشر الكتاب، وسحب نسخة من دور النشر، غير أنه في غضون أسبوع واحد من ذات الحكم وجد الكتاب منشورا في أكثر من موقع على شبكة الإنترنت. راجع: أحمد عبد الكريم سلامة:الإنترنت والقانون الدولي الخاص فراق أم تلاق، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من1-3مايو 2000، المجلد الثاني، ط3، 2000،ص29. وراجع:جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة،2002،ص7.

نقلها تتضمن استخدام تقنيات معلوماتية، وفي المقابل يجب السماح باستخدام تقنيات معلوماتية مضادة بهدف التنقيب والتحري والتحقيق في تلك الجرائم [1].

وبسبب تلك المشكلات المتعلقة بالجوانب الإجرائية للجريمة المعلوماتية فقد ظهرت العديد من الاتفاقيات والتوصيات الدولية بهدف معالجة تلك المشكلات، والحد منها قدر المستطاع، وصولا إلى إقرار تلك المبادئ أو الاستعانة بها في تشريعات الدول الموقعة على تلك الاتفاقيات، وبعض الدول الأخرى ومنها الجزائر[2]، ومع ذلك فلازال القصور يكتنف تلك التشريعات في ظل عدم وجود تعاون دولي في مكافحة هذا النوع من الإجرام، ولازالت القوانين الإجرائية لكثير من الدول، ومنها أغلب الدول العربية خالية من نصوص يتم التعامل من خلالها تقنيا في مجال التحري و الاستدلال، أو التحقيق، أو المحاكمة بما يتناسب مع الأساليب الفنية ذات الطابع التقني التي ترتكب بها تلك الجرائم.

ولإيضاح تلك المشكلات فسيتم الاقتصار في الفصل الأول من هذا الباب على المشكلات الإجرائية المتعلقة بالاستدلال والتحقيق، وفي الفصل الثاني نتناول المشكلات الإجرائية المتعلقة بالاختصاص القضائي، وحجية الدليل الالكتروني في الإثبات والتعاون الدولي في معالجة تلك المشكلات.

---

(1) هلالي عبد أللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23نوفمبر 2001، مرجع سابق، ص253.

(2) يعد التشريع الجزائري من التشريعات التي أولت اهتماما بالغا بالجوانب الإجرائية لجرائم المعلوماتية، حيث لم يقتصر الأمر على تعديلات قانون الإجراءات الجزائية أخرها تعديل 2006 بموجب القانون رقم (06- 22) المؤرخ في 20 ديسمبر 2006المٌعدِل والمٌتمِم للأمر رقم(66- 156) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية، وتضمينه بعض الصلاحيات المتعلقة بالاستدلال أو التحقيق في جرائم المعلوماتية ومنها تمديد الاختصاص القضائي، وعدم التقيد ببعض الضمانات الخاصة بالتفتيش أو الضبط مثل مواعيد التفتيش والأشخاص المطلوب حضورهم وغير ذلك، بل أنه قد عمل على إصدار قانون خاص يتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، وهو القانون رقم (09 - 04) المؤرخ في 5 غست (أغسطس) سنة 2009 ، والمنشور بالجريدة الرسمية رقم (47) الصادرة بتاريخ 2009/8/16، وتضمن هذا القانون العديد من الإجراءات والالتزامات ذات الطابع التقني والتي من خلالها يستطيع ضابط الشرطة القضائية أو قاضي التحقيق الوقاية والتعامل مع تلك الجرائم ومرتكبيها، ومنها مراقبة الاتصالات الإلكترونية، والقواعد الإجرائية لتفتيش نظم المعلوماتية، وحجز المعطيات المعلوماتية، والالتزامات التي تقع على مقدمي الخدمات في مساعدة السلطات المكلفة بالتحريات القضائية، وكذلك الالتزامات الخاصة بمقدمي خدمة الإنترنت، كما تضمن القانون إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الاتصالات ومكافحته وحدد مهامها ومنها:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصالات ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

وتضمن القانون في الفصل الأخير منه- السادس- التعاون والمساعدة القضائية الدولية إزاء تلك لجرائم.

الفصل الأول

الاستدلال والتحقيق

ظهرت المشكلات الإجرائية في مجال الجرائم المعلوماتية بسبب ارتباطها ببيانات معالجة معلوماتيا وكيانات منطقية غير مادية، وبالتالي صعوبة كشف هذه الجرائم من ناحية، واستحالة جمع الأدلة بشأنها في اغلب الأحيان من ناحية أخرى، ومما يزيد من صعوبة الإجراءات، سرعة ودقة تنفيذ الجرائم المعلوماتية، وإمكانية إزالة آثارها، وإخفاء الأدلة الناتجة عنها عقب ارتكابها مباشرة، حيث يواجه التحري وجمع الاستدلال، أو التحقيق إشكاليات كثيرة، تكمن في الطبيعة غير المادية للمعطيات المعلوماتية التي يكون لها دور في كشف الجريمة، وتبدو تلك المشكلات في صعوبة التفتيش على تلك المعطيات من خلال الأنظمة المخزنة بها، وكذلك تجميعها، وحفظها، وتخزينها، وحجزها عن طريق الإجراءات التقليدية المنصوص عليها في قوانين الإجراءات التقليدية، بحيث لم تعد تلك الإجراءات تتناسب مع الأساليب الحديثة لاقتراف تلك الجرائم، حيث تتطلب السرعة في مواجهتها قبل إزالة أثارها، أو التلاعب بالمعطيات التي يمكن أن تكون هي الدليل الوحيد في كشف الجريمة، والوصول إلى الجاني، ويتطلب الآمر القيام بإجراءات ذات طابع تقني تتضمنها القوانين الإجرائية، وتكون السلطة المعنية بالاستدلال أو التحقيق مدربة على القيام بها ومتابعة للجديد فيها.

كما أن تلك المشكلات تكون أكثر تعقيدا عندما يكون الإجراء المتخذ بصدد بيانات مخزنة في أنظمة أو شبكات موجودة بالخارج، فالطابع الدولي للفضاء الإلكتروني بتخطيه للحدود الدولية قد آثار العديد من المشكلات حيال جرائم تعدت الحدود بين الدول، حيث تثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها الاستدلال، أو التحقيق، مشكلات تتعلق بسيادة الدولة أو الدول التي توجد لديها هذه البيانات، في ظل عدم وجود الشرعية الإجرائية والتعاون الدولي لمكافحة تلك الجرائم.

لما تم ذكره فسيتم تناول المشكلات المتعلقة بالتحري والاستدلال في مبحث والمشكلات المتعلقة بالتحقيق في مبحث آخر.

المبحث الأول

التحري والاستدلال

تعد مرحلة جمع الاستدلال أو البحث التمهيدي من المراحل الهامة في بناء الدعوى الجنائية، لأنها هي المرحلة التي تسبقها، وتهدف إلى البحث عن الجرائم والكشف عنها وعن مرتكبيها[1]، وغالبا ما تقوم بتلك الأنشطة أجهزة الشرطة في مجال عملها كأجهزة ضبط قضائي[2] إذ يكون عملها سابقا للاتهام والتحقيق، وهو من مقدمتهما، ويلعب دورا مهما في تهيئة القضية للقضاء الجنائي بوجه عام[3].

وتقوم مهمة التحري وجمع الاستدلال على استقصاء الجرائم وتعقب مرتكبيها، ويكون ذلك بجمع كافة العناصر والقرائن والأدلة التي تفيد التحقيق في الدعوى، ولهم في سبيل ذلك أن ينتقلوا إلى مكان الواقعة لإثبات حالة الأشياء ورفع الآثار التي تخلفت عن الجريمة .

---

(1) إجراءات البحث والتحري لم يذكرها القانون حصرا، وإنما وضع قاعدة عامة تخول لمأمور الضبط أن يقوم بأي إجراء من شأنه الكشف عن الجريمة ومرتكبيها، وتعقبهم لتقديمهم للسلطة المختصة، أي القيام بأي إجراء من شأنه الكشف عن الجريمة ومرتكبيها وجمع أدلتها، وتتميز بعدم تعرضها للحقوق والحريات، فإجراءات الإستدلال ليس فيها تعرض للحقوق والحريات، نظرا لطبيعتها شبه القضائية.راجع: عبد الله أوهايبية، شرح قانون الإجراءات الجزائري، دار هومه للطباعة والنشر، الجزائر، 2005.ص11، وص12.

(2) بالإضافة إلى أن أجهزة الشرطة تقوم في مجال عمل الضبط القضائي وفقا لنصوص القانون الذي يحدد الفئة التي تتمتع بصفة مأموري الضبط القضائي وصلاحياتها، فإن أجهزة الشرطة تقوم بمهام أخرى في مجال الضبط الإداري وهي المرحلة السابقة لوقوع الجريمة، حيث يكون دورها في تنفيذ المهام المناطة بها في هذه المرحلة هو دور وقائي، يهدف إلى الحيلولة من وقوع الجرائم، وذلك عن طريق القيام بالعديد من المهام منها مراقبة تطبيق القوانين واللوائح، والدور الوقائي في الوقاية من جرائم المعلوماتية يتم عن طريق المراقبة الدورية لمحلات ترويج برمجيات الحاسبات الإلكترونية من خلال الاطلاع على الترخيصات القانونية، و بالتالي الوقوف في وجه الجريمة الإلكترونية، و التجارة غير المشروعة بالبرمجيات و الملفات المدمجة و غير المدمجة، كما يمكن القيام بدوريات في غرف الدردشة بغرض مراقبة ما يحدث فيها، وللضبطية الإدارية في هذه الحالة كافة الصلاحيات اللازمة للوقاية من كافة صور الإجرام الإلكتروني، كما تم تطوير برامج في مجال عمل الضبط الإداري، ومن تلك البرامج ما طرحته وزارة الأمن العام الصينية لإبعاد المعتقدات والجنس والعنف عن الإنترنت في الصين، وأطلق عليه أسم شرطة الإنترنت لمنع المستخدمين من تلقي معلومات ضاره من مواقع أجنبية، و إلى جانب هذه الإجراءات التي تتخذها شرطة المنع لمواجهة جرائم البيئة الإلكترونية مبكرا، و بالتالي منع وقوعها، هناك إجراءات يقوم بها العاملون بالمنشآت الحيوية يطلق عليها "أمن المعلومات"، و هي عبارة عن احتياطات و إجراءات تتخذها الإدارات الحديثة بالتعاون مع الأجهزة الأمنية لمنع وقوع الجريمة وذلك من خلال تحليل المخاطر والتهديدات، لتتم عملية اتخاذ الإجراءات المضادة و بالتالي الحيلولة دون وقوع الجريمة. ويأتي بعد الدور الوقائي الدور ألضبطي الهادف إلى الكشف عن الجريمة ومرتكبيها من خلال التحري والاستدلال. لمزيد من التفصيل حول الدور الوقائي للحيلولة دون اقتراف الجرائم راجع: محمد بن حاج الطاهر وعبد القادر دوحة، التحديات الأمنية والقضائية لمنع الجريمة الإلكترونية، بحث مقدم إلى الملتقى الوطني الأول - القانون وقضايا الساعة- النظام القانوني للمجتمع الالكتروني، المركز الجامعي، خميس مليانه، ولاية عين الدفلى، الجزائر، من9: 11 مارس 2008، ص168، وراجع جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق،ص11ومابعدها، وراجع أيضا: أحسن مظفر الرزو، ((الأمن ألمعلوماتي معالجة قانونية أولية))، مجلة الأمن والقانون، صادرة عن أكاديمية شرطة دبي، الإمارات العربية المتحدة، ع1، س12، يناير 2004، ص70 وما بعدها.

(3)عبد الله أوهايبية، مرجع سابق، ص184.

ومع ذلك فتحظر على مأموري الضبط القضائي القيام بأمور معينة أثناء جمع الاستدلال ومنها تحليف الشهود اليمين إلا إذا خيف عدم استيفاء الشهادة فيما بعد.

أو القيام بعملية التفتيش أو الضبط، وكذلك الاستجواب، وغير ذلك من إجراءات التحقيق إلا ما استثني بنص كما في حالة الجريمة المشهودة.

وحظر قيام مأموري الضبط القضائي من القيام بتلك الأعمال بسبب أنها تتعرض لحقوق وحريات الأفراد، لذلك فلا بد من ضمانات تتمثل في صفة القائمين بها وهي سلطة التحقيق، وضمانات أخرى ترافق القيام بتلك الإجراءات كحضور محامي المتهم وحضر القيام ببعض تلك الإجراءات خلال مواعيد زمنية معينة.

ويطلق على سلطات الضبط القضائي في القانون اليمني مأموري الضبط القضائي وفي القانون الجزائري ضباط الشرطة القضائية وأعوان الضبط القضائي[1].

---

[1] تضمنت المادة(84) إ.ج.ي رقم (13) لسنة 1994 تحديد مأموري الضبط القضائي بأعضاء النيابة العامة، والمحافظـــون، ومديرو الأمن العام، ومديرو المديريات، وضباط الشرطة والأمن، ورؤساء الحرس والأقسام ونقط الشرطة ومن يندبون للقيام بأعمال الضبط القضائي من غيرهم.، وعقال القرى، ورؤساء المراكب البحرية والجوية، وجميع الموظفين الذين يخولون صفة الضبطية القضائية بموجب القانون، وأية جهة أخرى مكلفة بالضبط القضائي بموجب قانون.

وتضمنت المادة (14) إ.ج.ج تحديد الذين يمكن إضفاء صفة الضبط القضائي عليهم وفقا لقواعد محددة وهم ضباط الشرطة القضائية، وأعوان الضبط القضائي، والموظفون والاعوان المنوط بهم قانونا بعض مهام الضبط القضائي، وجاءت المادة (15) وحددت من تثبت لهم صفة ضباط شرطة قضائية، وكذك المادتان (19 ،و20) حددت طائفة الاعوان، وحددت المادتين (21، 28) طوائف الموظفين الموكل لهم بعض اعمال الضبط القضائي، واحالة المادة 27 على القوانين الخاصة إمكان إضفاء صفة الضبطية القضائية على الموظفين والاعوان، وطبقا للمادة(15)فإنه يتمتع بصفة ضباط الشرطة القضائية كلا من: رؤساء المجالس الشعبية، وضباط الدرك الوطني، ومحافظو الشرطة، وضباط الشرطة، و ذوي الرتب في الدرك، ورجال الدرك الذين امضوا في سلك الدرك ثلاث سنوات على الاقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني بعد موافقة لجنة خاصة، ومفتشوا الامن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الاقل وعينوا بموجب قرار مشرك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية بعد موفققة لجنة خاصة، وضباط وضباط الصف التابعين للمصالح العسكرية للامن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل. اما اعوان الضبط القضائي فقد نصت عليهم المادة(19) من الأمر رقم (95- 10) المؤرخ في 25فبراير 1995وهم: موظفوا مصالح الشرطة، وذو الرتب في الدرك الوطني، رجال الدرك الوطني، ومستخدمي مصالح الامن العسكري، واعضاء الحرس البلدي بموجب المرسوم التنفيذي رقم(96- 266)المتعلق بالقانون الاساسي للحرس البلدي. وبالنسبة للاعوان والموظفون المكلفون ببعض مهام الضبط في ق.إ .ج.ج فهم فئة الموظفين والاعوان المختصين في الغابات وحماية الاراضي واستصلاحها وفقا للمادة(21)، وولاة الولايات في حالة الاستعجال، أو في حالة وقوع جناية أو جنحة تمس أمن الدولة (مادة 28)إ.ج.ج . اما مأموري الضبط في القوانين الخاصة فهم : مفتشوا العمل، واعوان الجمارك المهندسون ومهندسوا شغال ورؤساء المقاطعة، واعوان الصحة النباتية، واعوان البريد والمواصلات السلكية واللاسلكية، راجع عبدالله أوهايبية، مرجع سابق، ص202 وما بعدها.

وعملية التحري الرقمي تختلف عن التحري في الجرائم المعتادة المرتكبة بالوسائل التقليدية، حيث تتعامل مع وسائط وأجهزة رقمية وأدلة غير ملموسة، ويكون من مهام أجهزة التحري تحديد من قام باختراق النظام، وكيف تم هذا الاختراق، ومدى الأضرار الناتجة عن هذا الاختراق، وفقا لمعايير وأطر عملية تمنع فقدان ومسح الأدلة[1].

ومع أن هذه المرحلة- التحري والاستدلال- لها أهمية كبيرة في كشف غموض الجريمة المرتكبة باستخدام الوسائل التقليدية وصولا إلى مقترفيها.

فإن تلك الأهمية تبدو أكثر إلحاحا في ظل اقتراف تلك الجرائم بالوسائل الإلكترونية الحديثة، بل وظهور جرائم جديدة ظهرت بظهور التكنولوجيا الرقمية.

ذلك أن اقتراف هذه الجرائم بما فيها المستحدثة إنما تقترف بوسائل وأساليب حديثة، وذلك ما يجعل إجراءات مرحلة جمع الاستدلال بشكلها التقليدي قد لا تفي بمواجهة تلك الجرائم إجرائيا، وقد تحتاج إلى قواعد إجرائية تتناسب مع حداثة الجريمة وتتغلب على المشكلات التي تثيرها فما هي المشكلات الإجرائية التي تعيق مرحلة التحري و الاستدلال؟

([1])سلطان محيا الديحاني، التحري في الجريمة المعلوماتية، جريدة القبس الكويتية، ع 12392 نوفمبر2007، ت.د 2008/1/20 على الرابط:
http://www.alqabas.com.kw/Final/NewspaperWebsite/NewspaperPublic/ArticlePage.aspx?ArticleID=230005

المطلب الأول

التعامل مع البلاغات والشكاوي عبر الإنترنت

تضمن التشريع اليمني والتشريع الجزائري النص على إلزام مأموري الضبط القضائي بالتحري عن الجريمة والكشف عن مرتكبها، وتلقي البلاغات والشكاوي وفحصها، والانتقال إلى مكان حدوث الجريمة للمعاينة والحفاظ على الأدلة واخذ أقوال المتواجدين في مكان الحادث [1].

وتأتي أهمية البلاغ في أنه يعد بمثابة إشعار للسلطة بأن جريمة ما قد وقعت ويجب التحرك لمواجهتها، وللمجني عليه وأفراد المجتمع دور لا يستهان به في الإبلاغ عن الجريمة، لأنهم هم من يشعرون السلطة المختصة بوقوع الجريمة، إضافة إلى الجرائم التي يتم الإبلاغ عنها من قبل أجهزة التحري.

ويجب على مأمور الضبط القضائي فور تلقي البلاغات والشكاوي تدوينها والتأكد من صحتها، ومن ثم اتخاذ كافة الإجراءات التالية لها، من الانتقال إلى مكان الجريمة للمحافظة عليه من التلاعب بمحتوياته، وإثبات الحالة، وسماع أقوال المشتبه فيهم والشهود، وعمل محاضر بذلك.

وإذا كان تلقي البلاغات والشكاوي قد يبدو سهلا في مجال الجريمة التقليدية، فقد لا يكون كذلك في مجال الجريمة المعلوماتية حيث تثار مسألة مدى إمكانية تلقي البلاغات والشكاوي عن طريق الإنترنت ونظم المعلوماتية، ومن ثم التحقق منها والحصول على استيضاحات بشأنها.

فالمشكلة تكمن إذن في مدى إمكانية قيام الضبطية القضائية- الشرطة القضائية- بتلقي وقبول البلاغات عبر الإنترنت، وما هي القيمة القانونية لمثل هذا النوع من البلاغات وموقف القانونين اليمني والجزائري منها؟

ولإيضاح مدى قبول تقديم البلاغ أو الشكوى عبر الإنترنت يلزم التطرق إلى مدى أهمية البلاغ عبر الإنترنت للتعرف عما إذا كان هناك اختلاف في أهميته عما هو الحال

([1]) راجع: المادة (91) من القانون رقم (13)لسنة 1994 بشأن الإجراءات الجزائية اليمني، والمادة (17) من القانون الجزائري رقم (01-08)المؤرخ في .26 يونيو 2002 المُعَدِلْ والمُتَمِمْ لقانون الإجراءات الجزائية، (ج.ر 34، ص5)، وانظر الجريدة أيضا في موقع وزارة العدل الجزائرية، ت.د 20/ 10/ 2007على الرابط. http://www.joradp.dz/TRV/APPenal.pdf

عليه في العالم المادي، وهل يُكتفى بالنصوص الخاصة في القوانين الإجرائية التقليدية أم أن الوضع يحتاج إلى نص خاص يتضمن تقديم البلاغ والشكوى عبر الإنترنت؟

وبهذا الخصوص يمكن القول بأن البلاغ أو الشكوى عبر الإنترنت لا يمثلان مشكلة تعيق إجراءات التحري والاستدلال في البلدان المتقدمة التي أضحت توجد بها أجهزة متخصصة لتلقي البلاغات والشكاوي عبر الإنترنت ومتابعتها واتخاذ الإجراءات اللازمة بشأنها [1]، وإذا وجدت مشكلة مرتبطة بالبلاغ في تلك الدول فهي تعود إلى الجهة التي ارتكبت الجريمة حيالها، سواء كانت تلك الجهات أشخاص أو مؤسسات، وذلك بعدم قيام تلك الجهات بالإبلاغ عن الجرائم المعلوماتية المرتكبة بحقها خوفا على سمعتها وحتى لا تتضرر بسبب ذلك [2].

بينما يعد تقديم البلاغ والشكوى عن طريق الإنترنت مشكلة في البلدان التي لازالت متأخرة في مجال التقدم التكنولوجي، لعدم وجود مواقع وأجهزة متخصصة بهذا الخصوص، وحتى في حالة وجود مواقع للإبلاغ عبر الإنترنت فإنه لا يتم تفعيل العمل بواسطتها لتلقي البلاغات بسبب عدم وجود الكوادر المتخصصة في هذه الدول، إضافة إلى قصور الخبرة الفنية والتقنية، بل والتعامل مع الحاسوب والإنترنت لدى مأموري الضبط القضائي في مجال الاستدلال في الجريمة المعلوماتية.

و من حيث أهمية البلاغ والشكوى عبر الإنترنت ونظم المعلوماتية فهي لا تقل عن أهميتهما في العالم المادي، ذلك أن الهدف هو إيصال المعلومة إلى مأمور الضبط القضائي بأن جريمة ما قد وقعت، وهذا العلم يتأتى سواء باستخدام الطرق التكنولوجية أو التقليدية، لذلك لا يشترط في مقدم البلاغ صفة معينة، فقد يكون هو المجني عليه وقد يكون فردا من عامة الناس، وذلك لا يتنافى مع كون البلاغ قد تم عن طريق الإنترنت أو بالطرق التقليدية، لأن العبرة في صحة الواقعة في نهاية الأمر يعود إلى ما تقتنع به المحكمة [3].

---

(1) نشط عمل الضبطية القضائية عبر الإنترنت، بحيث أصبح من الممكن تقديم البلاغ أو الشكوى عبر مواقع متخصصة بهذا الشأن مثل مواقع المباحث الفدرالية الأمريكية FBI، ووزارة العدل الأمريكية USDOJ و المخابرات المركزية الأمريكية CIA، وكذلك موقع حماية البرمجيات الأوربية APP، حيث يناط بمثل هذه الجهات وغيرها تلقي البلاغات والشكاوي، سواء تعلقت بجريمة تقليدية أو معلوماتية. راجع: عمر محمد أبو بكر يونس الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص824.

(2) عفيفي كامل عفيفي، مرجع سابق، ص356.

(3) حسني الجندي، شرح قانون الإجراءات الجزائية اليمني، بدون دار النشر، بدون رقم الطبعة،1990، ص385.

ومع ذلك فإن البلاغ عبر الإنترنت ينطوي على جهالة أكثر مما هو عليه الحال في العالم المادي، وذلك بسبب أن البلاغ عبر الإنترنت يعتمد على نماذج جاهزة موجودة في مواقع الجهات المعنية، مثل موقع (FBI)، ولذلك فقد يكون المبلغ مجهولا في اغلب الأحوال، بالإضافة إلى أن البلاغ قد يكون غير صحيح، وبالتالي فإن المبلغ قد يفلت من العقاب في حالة البلاغ الكاذب عن طريق الإنترنت أكثر مما هو عليه الحال في العالم المادي[1].

ويترتب على ما سبق في أن الإشكالية لا تكون في تلقي البلاغ وقبوله، والقيمة القانونية له، بقدر ما تكون في السلطة المختصة بتلقي البلاغات والشكاوي، فإذا كانت سلطة مختصة يخول لها القانون إجراءات تتناسب مع حداثة الجريمة، ابتداء من تلقي البلاغ وانتهاء بضبط أدلة الجريمة فلا مشكلة في تلقي البلاغ أو الشكوى في مجال العالم الرقمي، وإذا كانت تلك الجهة غير مختصة ولا توجد نصوص قانونية تخول لها اتخاذ إجراءات تتناسب مع تلك الجرائم، فإن مسألة تلقي البلاغ وقبوله لن تلاقي نفس الاهتمام السابق، ذلك أن هذه الجهة وإن تلقت البلاغ فإنها ستكون عاجزة عن اتخاذ أية إجراءات فنية وتقنية لملاحقة الجريمة وضبطها.

كما أن من المشكلات التي قد تثار بصدد الشكوى في أن الشكوى لا تقبل إلا من مدعي بحق مدني أو مضرور، بينما الشكوى عبر الإنترنت ونظم المعلوماتية قد تقدم من شخصية لا تحمل الاسم الحقيقي لها.

بالإضافة إلى أن المجني عليه في جرائم البث العلني قد يتلقى سباً أو تشهيراً عبر الإنترنت، وهو يستخدم اسم مستعار أو صفة غير حقيقية ، وبهذا الشأن فإن القضاء في بعض الدول قد أقر قبول الشكوى من المجني عليه حتى لو كان يستخدم اسماً وهمياً أثناء تعرضه للتشهير أو السب[2]، كما لو كان في حلقة نقاش في الإنترنت وهو يستخدم اسماً مستعاراً ، أو أن الوقائع التي تعرض للشتم بسببها وهمية، إلا أن مثل هذا الرأي لا يخلو من النقد لكون ذلك يفتح المجال في تلقي الشكاوى من كل من يحمل اسما وهميا أو

([1])عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 830.

([2])أخذ القضاء الاسترالي بالرأي القائل بقبول الشكوى عبر العالم الافتراضي من الشخص الذي كان يستخدم اسم مستعار أو شخصية وهمية وذلك في قضية (Rindos v Hardwick)حيث اعتبرت المحكمة العليا لغرب استراليا في حكمها بتاريخ 1994/3/31 أن بث نقد لاذع لعدد 23000مشترك في BBS خاصة بمؤسسة تعليمية متخصصة، في الوقت الذي تعد فيه حلقة النقاش متوفرة عالميا، مظهرا من مظاهر التشهير.راجع :عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص836.

مستعار، وذلك يتعارض مع كون الشكوى لا تقبل إلا من متضرر، ولابد في أن يكون ذلك المتضرر معروفا وهو الذي يتقدم بتلك الشكوى.

كما أن الإقرار بقبول الشكوى من الشخص الذي تعرض لجرائم البث العلني أثناء اتخاذه اسما وهميا أو مستعاراً في وقت ما كان في إحدى حلقات النقاش عبر الإنترنت يتيح المجال أمام الجميع في التعامل بأسماء شخصيات وهمية، ومثل هذا الأمر يجعل الشخصية الوهمية في حالة مشروعية دائمة[1]، ولا يفرق بين ما إذا كان الغرض من استخدام الاسم المستعار أو الوهمي مشروعا أم لا، حيث يكون مشروعا إذا كان القانون يسمح بذلك [2].

ومع أنه لا يوجد نصوص في القانونين اليمني والجزائري تتضمن تقديم البلاغ أو الشكوى عبر الإنترنت، والاكتفاء بالنصوص التقليدية، حيث تضمن قانون إ.ج.ي النص على اختصاص مأموري الضبط القضائي بفحص البلاغات والشكاوى وجمع الاستدلالات والمعلومات المتعلقة بها وإثباتها في محاضرهم وإرسالها إلى النيابة العامة[3]، وحث كل من علم بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو إذن، أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي بها [4].

([1])عمر محمد أبو بكر يونس، المرجع السابق، ص836.

([2]) يتيح القانون الجزائري لمأموري الضبط القضائي في بعض الحالات استخدام الاسم الوهمي أو المستعار تحت مسمى التسرب إذا استدعت ضرورة التحري أو التحقيق ذلك، على أن يكون ذلك في إحدى الجرائم المنصوص عليها في المادة (65 مكرر 5) إ. ج. ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والجرائم المنظمة العابرة للحدود الوطنية وجرائم الإرهاب، وجرائم المخدرات، وجرائم تبييض الأموال، وجرائم الفساد، والجرائم المتعلقة بالتشريع الخاص بالصرف الصحي، بعد أخذ الإذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية وتحت رقابته، ويقصد بالتسرب مراقبة الأشخاص المشتبه بارتكابهم إحدى الجرائم المذكورة بحيث يسمح لمن يقوم بالمراقبة –سواء كان ضابط شرطة قضائية أو عوناً يعمل تحت إشرافه- اتخاذ اسم وهمي أو مستعار بغرض ضبط الجريمة، وفي هذه الحالة يكون التخفي تحت الاسم الوهمي أو المستعار عملا مشروعا بموجب القانون، وإذا تعرض مأمور الضبط للسب أو إحدى جرائم البث العلني، فإنه يكون من حقه أن يتقدم بشكوى مع أنه تعرض لذلك أثناء قيامه بمهامه وهو يتخذ اسما وهميا أو مستعاراً كون استخدام ذلك الاسم كان مشروعا، وذلك ما يتعارض مع أصحاب الرأي القائل بقبول الشكوى من صاحب الاسم الوهمي دون أن يميزوا ما إذا كان استخدام ذلك الاسم قد تم بصورة مشروعة، أم لا.لمزيد من التفصيل حول التسرب راجع المواد من (65 مكرر 11 : 65 مكرر 18)من القانون (رقم 06 – 22)المؤرخ في 20 ديسمبر 2006المُعَدِلْ والمُتَمِمْ لقانون الإجراءات الجزائية، الجريدة الرسمية رقم (84 بتاريخ 24 ديسمبر 2006، ص4)، كما تجد الجريدة الرسمية منشورة على موقع وزارة العدل الجزائرية، ت.د14 /2009/1، على الرابط:
http://www.joradp.dz/TRV/APPenal.pdf

([3])راجع المادة(91) إ.ج.ي .

([4])راجع المادة (94) من نفس القانون.

كذلك فقد تضمنت المادة (17) إ.ج.ج على مهام ضباط الشرطة القضائية ومنها تلقي الشكاوي والبلاغات والقيام بجمع الاستدلالات وإجراء التحقيقات الابتدائية [1].

وقد جعل القانونان البلاغ وجوبياً في حال أن يعلم أي من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأديتهم لعملهم أو بسبب ذلك، بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو إذن[2]، وكذلك يجب على كل سلطة نظامية وكل ضابط أو موظف عمومي يصل إلى علمه أثناء مباشرته مهام وظيفته خبر جناية أو جنحة إبلاغ النيابة العامة بدون توان، وأن يوافيها بكافة المعلومات، ويرسل إليها المحاضر والمستندات المتعلقة بها[3].

ومع أن القانونين قد تضمنا كيفية تقديم البلاغات والشكاوي بالوسائل التقليدية، إلا أن ذلك لا يعد مانعا من تقديمهما عبر الإنترنت، لأن الخلاف يكمن في الوسيلة فقط، بين أن تكون الوسيلة التي تم الإبلاغ بواسطتها تقليدية، أو إلكترونية .

كما أن النصين في كلا القانونين تضمنا لفظ "تلقي البلاغات والشكاوي " ولم يجعلا ذلك مقتصرا على الوسائل التقليدية فحسب، إذ ورد اللفظ عاما ولم يحدد وسيلة بذاتها يقتصر الإبلاغ أو تقديم الشكوى بواسطتها، مما يتيح المجال أمام تطبيقهما على تقديم البلاغ أو الشكوى عن طريق وسائل المعلوماتية.

وبناء على ما سبق فإنه لا يوجد ما يحول من قبول البلاغ أو الشكوى عبر الإنترنت في القانونين اليمني والجزائري، وفقا للنصوص القانونية القائمة، وكل ما في الأمر تدريب شرطة متخصصة للعمل في ذات المجال تستطيع التعامل مع الأجهزة والبرامج المخصصة لمثل تلك المهام، أسوةً بالدول السباقة في هذا المجال.

ومع ذلك فإن على المشرعين في كلا البلدين تضمين قانوني الإجراءات الجنائية في المواد الخاصة بالإبلاغ عبارة "بأية وسيلة كانت" سدا للذرائع وبهدف معالجة الإشكالية الخاصة بتقديم البلاغ أو الشكوى من كل من يحمل اسماً وهمياً، وذلك بالنص على عدم قبول الشكوى طالما لم تقدم من صاحب شأن أو مضرور، بخلاف البلاغ الذي يمكن قبوله من الشخص حتى لو كان يحمل اسماً وهمياً ، لأنه سوف يخضع للفحص

---

(1) راجع لمادة (17) إ.ج.ج رقم (01- 08) المؤرخ في 26يونيو لسنة 2001 (ج.ر 34.ص5).

(2)راجع: المادة (95) من نفس القانون.

(3)راجع: المادة(32) إ.ج.ج.

والتأكد من صحته، إضافة إلى أن قبوله سيخدم الأمن الوقائي للمجتمع من الوقاية من حدوث آي جريمة محتملة.

ومع ذلك فإن المشكلة الأهم في ما يخص الإبلاغ بجرائم المعلوماتية سواء تم الإبلاغ بالطرق لتقليدية، أو عن طريق الإنترنت تتمثل في الإحجام عن تقديم البلاغ إزاء تلك الجرائم من الأشخاص والمؤسسات التي تضررت من تلك الجرائم بسب الخوف من اختلال الثقة التي تتمتع بها وما سيترتب على ذلك من أثر سلبي على التعامل معها[1].

المطلب الثاني

الاختصاص المكاني

تعتبر مشكلة الاختصاص المكاني للجرائم المعلوماتية ذات أهمية كبيرة في عرقلة الإجراءات الخاصة بأجهزة الضبط القضائي، عند مقارنتها بالإجراءات المتخذة بصدد الجريمة التقليدية، ذلك أنه في الجريمة التقليدية تكون إجراءات مأمور الضبط القضائي محددة بالاختصاص المكاني الذي يمارس عمله منه، وبالتالي فإن أي تجاوز في الإجراءات لذلك الاختصاص- ما لم يستثن القانون حالات معينة- يكون مصيره البطلان، وإذا كان مأمور الضبط يتمتع بالصلاحيات الممنوحة له قانونا في نطاق اختصاصه، ولايحق له تجاوز ذلك الاختصاص في مجال جمع الاستدلال والتحري الهادف إلى كشف الجريمة التقليدية، فإن الأمر في مجال الجرائم المعلوماتية يحتاج إلى إعادة النظر، لأن اقتراف تلك الجرائم فيه تجاوز للحدود الجغرافية، وتحتاج في متابعتها

---

(1) ومن الأمثلة على الإحجام في الإبلاغ عن الجرائم المعلوماتية، قيام مدير المبيعات بإحدى الشركات الانجليزية باستخدام أسماء وهميه لشركات في حاسبات الشركة التي تجري معالجتها عن طريق الحاسب، وعن طريق برنامج تم وضعه يتم عمل شيكات بأسماء الشركات الوهمية يقوم هو فيما بعد بالاستيلاء عليها، وبعد أن تكشف التلاعب الذي يقوم به في حاسبات الشركة وبدلا من الإبلاغ به بسبب خوف الشركة على سمعتها أثناء المحاكمة، إذا بالشركة تقوم بعمل توصيه له لمساعدته في إيجاد عمل له مدير تنفيذي، ويتمكن بواسطتها من العمل في شركة أخرى ويكرر نفس العمل – الجريمة- الذي قام به في الشركة الأولى حيث قام باختلاس مبلغ 350.000 $، ويتكرر نفس الإجراء من الشركة الثانية في الإحجام عن الإبلاغ خوفا على سمعتها والرضوخ إليه بعمل توصيه لمساعدته على العمل، ولم يكتف بذلك بل طالب الشركة بتعويضه مبلغ 6000$ على فقد وظيفته. راجع: منير الجنبيهي ومحمود الجنبيهي، بروتوكولات وقوانين الإنترنت، دار الفكر الجامعي الإسكندرية، بدون رقم وتاريخ الطبعة، ص376. وكذلك راجع محمد الأمين البشيري،((التحقيق في جرائم الحاسب الآلي والإنترنت)) المجلة العربية للدراسات الأمنية والتدريب، صادرة عن أكاديمية نايف للعلوم الأمنية، الرياض،ع30، نوفمبر2000، ص350.

وكشفها تعدي تلك الحدود في مجال العالم الرقمي، ومعلوم بأن أي إجراء يقوم به مأمور الضبط القضائي خارج نطاق اختصاصه يكون معرضا للبطلان .

ومع ذلك فقد وجدت تطبيقات قضائية ورأي فقهي اعتبرت بأن قيام مأموري الضبط القضائي بالحصول على معلومات عن طريق الهاتف أو الفاكس من خارج نطاق اختصاصه آمراً لايشوبه البطلان [1]، وتبريرذلك بأن تلك المعلومات تأتي إلى المأمورولا يذهب إليها، كما أنه لاينتقل انتقالا ماديا يخرجه من دائرة اختصاصه المكاني، وإنما انتقالا افتراضيا لاعلاقة له بالاختصاص المادي.

ولاأتفق مع اصحاب هذا الإتجاه، ففي جرائم المعلوماتية وإن كان الأمر لايتعلق بالانتقال المادي لمأمور الضبط القضائي، وإنما انتقال رقمي لاتوجد فيه حدود جغرافية بموجبها يمكن الالتزام بقاعدة الاختصاص المكاني، إلا أن ذلك الإنتقال يتسبب في إحداث مشكلة تتمثل في التعدي على سيادة الدول، أو الدولة التي تم الانتقال اللامادي إلى النظام الموجود فيها، إذا ماقام مأمور الضبط القضائي أثناء عمله بتجاوز الاختصاص المكاني وفقا للقواعد التقليدية.

وبالتالي فإن المسألة معقدة وتحتاج إلى تعاون دولي لحل هذه الإشكالية، لكي يتمكن مأمور الضبط من الخروج عن قاعدة الاختصاص المكاني عبر العالم الرقمي في الوقت الذي يكون موجودا ماديا في نطاق اختصاصه.

([1]) ففي إحدى القضايا في فرنسا و التي ترجع إلى 10 يناير 1992 كان مأمور الضبط القضائي يتلقى تلفونات وفاكسات من خارج نطاق دائرة اختصاصه تتضمن معلومات مفيدة للتحقيق الاولي Enquète préliminaire الذي كان يتولاه، وكان يدون المعلومات التي يتلقاها تلفونيا أو بالفاكس في محاضر جمع الاستدلال، فما كان من المتهم إلا أن قام بالطعن أمام غرفة الاتهام في بطلان إجراءات مأمور الضبط بحجة ممارستها من خارج نطاق اختصاصه الإقليمي ومخالفة الاحكام الخاصة بسماع شهادة الشهود، إلا أن غرفة الاتهام رفضت هذا الطعن، حيث رأت أن الإجراءات التي قام بها المأمور لاتعني انتقاله خارج نطاق إختصاصه الذي يمارس فيها وظائفه عادة، كما لايمكن تشبيه المعلومات التي ترد عن طريق التليفون أو الفاكس بشهادة الشهود، وإنما هي مجرد رسائل لاتعدو قيمتها عن مجرد معلومات تخضع لرقابة وتقدير قاضي التحقيق، وتلى ذلك أن قام المتهم بالطعن بقرار غرفة الإتهام أمام محكمة النقض والتي بدورها رفضت الطعن، على أساس أنه طبقا للمادة 1/18 إ.ج.فإن مأموري الضبط القضائي ليس لهم اختصاص - من حيث المبداء – إلا في حدود دائرة اختصاصهم الاقليمي، حيث يمارسوا وظائفهم المعتادة، فليس هناك مايمنعهم من جمع المعلومات من خارج دوائر اختصاصهم بواسطة التليفون أو الفاكس أو أي وسيلة أخرى للاتصال، حيث أن قيمة المعلومات التي يتم جمعها بهذه الطرق تخضع للمناقشة الحضورية للاطراف وتخضع لتقدير محكمة الموضوع، وطبقا لهذا فإن الانتقال غير المادي للمعلومات من مكان يقع خارج الحدود الاقليمية لإختصاص مأمور الضبط القضائي إلى دائرة اختصاصه لايخالف القانون وبالتالي يمكن الاعتماد عليه كدليل اثبات حسب راي- المؤلف الذي أورد القضية- جميل عبد الباقي الصغير، ادلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص102، وص103.

وعلى ضوء التعاون الدولي لابد من تقرير نصوص خاصة تعالج هذه المسألة التي هي على قدر كبير من الخطورة في مجال عمل الضبط القضائي، وذلك ماتم تداركه على مستوى الاتحاد الأوربي[1].

فمع تميز جرائم المعلوماتية بالعالمية، أي بكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، ووضع ترتيبات فعالة للمساعدة القانونية المتبادلة permettent une coopération directe entre plusieurs pays et تتيح التعاون المباشر بين عدة بلدان و création de réseaux intergouvernementaux pour les شبكات دولية[2] بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها[3].

وإذا تم حل مثل هذه الإشكالية في الدول المتقدمة تكنولوجيا ولو بشكل جزئي، كما في دول الاتحاد الأوربي وغيرها والتي اضحى لها تشريعات في هذا الخصوص[4]، فإن الوضع لايزال مثلما هو عليه في كثير من الدول ومنها أغلب الدول العربية، والتي لازالت تشريعات البعض منها تفتقر إلى نصوص قانونية لتنظيم التعامل مع تلك الجرائم في شقها الموضوعي، ناهيك عن افتقارها لنصوص تنظم المسألة في شقها الإجرائي، وان وجدت نصوص في بعض تلك التشريعات فما زال يعتريها النقص والقصور،

([1]) اتخذت الدول الأوربية خطوات جريئة في مجال مكافحة الجرائم المعلوماتية ضمن خطة أعدت لهذا الأساس، حيث وسعت من صلاحيات مأموري الضبط- أجهزة الشرطة- خارج النطاق المكاني لممارسة اختصاصهم بين الدول الأعضاء، وقد حظيت الخطة بدعم وزراء الاتحاد الأوروبي في اجتماع تقرر فيه أيضا منح مبلغ 300 ألف يورو لإنشاء جهاز لتجميع تقارير الإجرام وإصدار تحذيرات حول الأخطار المحدقة، كما دعم الاجتماع الوزاري إستراتيجية مكافحة الجريمة الإلكترونية التي ستنشئ فرق تحقيق تعمل عبر الحدود، و ترخص استخدام دوريات افتراضية لضبط بعض النواحي في الإنترنت، ومن "الإجراءات العملية " الأخرى تبادل أفضل للمعلومات بين قوات الشرطة في الدول الأعضاء في الاتحاد والشركات الخاصة حول طرق التحقيق واتجاهاته. راجع: موقع lazeeez، شبكة الإنترنت ،س. د 12،الأحد/2008/12/21على الرابط

http://lazeeez.com/qalam/i-424-2342.html

([2]) Guy de Vel: Les défis de la cybercriminalité, étude réalisé à l'occasion de la conférence sur les défis de la cybercriminalité, organisée par le conseil de l'europe, Strasbourg, les 15-17 Septembre2007.P.7.
http://www.nouvellesmenaces.com/images/userFiles/Gendarmerie/File/Defis%20de%20la(%20cybercriminalite%202004.pdf

[3] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998، ص 75.

(4) لا يمكن معالجة مشكلة تجاوز الاختصاص المكاني بشكل كلي عن طريق التعاون الدولي بسبب أن ما يعد جريمة في دولة معينة قد لا يعد كذلك في دولة أخرى، بالإضافة إلى تجريم بعض الدول لتلك الجرائم بنصوص جديدة بينما لا تزال دول تحاول تطبق النصوص التقليدية، مع أن ذلك يتصادم مع مبدأ الشرعية أحيانا، واختلاف النصوص بين الدول يعد عائقا في مجال التعاون الدولي، أضف إلى ذلك أن الدول المهيمنة في مجال التكنولوجيا الرقمية تحاول السيطرة الكاملة في مجال ملاحقة وضبط تلك الجرائم، لامتلاكها كل ما يخدم الجوانب التقنية في كشف تلك الجرائم بحيث تقوم باتخاذ الإجراءات دون مراعاة لتجاوز اختصاص ودون انتظار لموافقة الآخرين على قيامها بتلك الإجراءات في نطاق اختصاصهم.

بالإضافة إلى عدم وجود اتفاقيات عربية على مستوى الدول العربية، أوالانضمام إلى إتفاقيات دولية تنظم مكافحة هذه الجرائم .

وبالرجوع إلى القانون اليمني يلاحظ بأنه لم يتضمن نصا قانونيا ينظم امتداد إختصاص مأموري الضبط القضائي في بحث وتحري الجرائم المعلوماتية في النطاق الاقليمي، وحتى النصوص التي وردت في الاختصاص القضائي –اختصاص المحاكم - بإعتبار أن اختصاص مأموري الضبط القضائي يتبع الاختصاص القضائي للمحاكم فهي كذلك لم تنص بصورة صريحة على امتداد ذلك الاختصاص فيما يخص البحث والتحري في الجرائم المعلوماتية.

وبالعودة إلى تلك النصوص فإنه يتحدد الاختصاص المكاني لمأموري الضبط القضائي بإحدى أماكن ثلاثة هي:

مكان وقوع الجريمة، أو مكان إقامة المتهم، أو مكان القبض عليه [1]، وهي ذات الضوابط المحددة لتحديد الاختصاص في القانون الجزائري [2].

ويترتب على الخروج على القواعد السابقة لتحديد الاختصاص تعرض إجراءات مأموري الضبط القضائي للبطلان.

ومع ذلك فهذا الحكم لا يؤخذ على إطلاقه، حيث يجوز الخروج عن تلك القواعد في حالتين[3]:

الأولى: عندما يكون الإجراء متصلا بجريمة داخلة في اختصاص مأمور الضبط القضائي، ومثال ذلك عندما يقوم مأمور الضبط القضائي بتفتيش منزل المتهم الذي يقع خارج نطاق اختصاصه المكاني متى كانت الجريمة مرتكبة في نطاق اختصاصه، أو تم القبض عليه في تلك الدائرة، فإن التفتيش يكون صحيحا منتجا لأثاره مادام وله علاقة مباشره بالمتهم الذي ضبط متلبسا بالجريمة، وبموجب ذلك فإن الاختصاص يمتد إلى الذين اشتركوا في الجريمة.

والثانية: تتمثل في حالة الضرورة وتنقسم إلى قسمين:

---

(1) راجع المادة(234)إ.ج.ي رقم (13) لسنة 1994.
(2) راجع المادة (37)إ.ج.ج رقم(14- 04) المؤرخ في10نوفمبر2004(ج.ر 84 ،ص5)
(3) محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، ط1، بدون دار نشر، 2000م، ص38، وص39.

الأول:عند مصادفة المأمور للمتهم المأذون له قانونا بتفتيشه خارج نطاق اختصاصه المكاني وبدا له من مظهره والأفعال التي يقوم بها أنه يحوز دليل الجريمة، كالمادة المخدرة مثلا.

والثاني: يتعلق بمتهم هارب من تنفيذ العقوبة ويستلزم القانون تعقبه لتنفيذ العقوبة المحكوم بها ولو تجاوز في ذلك الاختصاص المكاني للقائم بالمطاردة.

وخلاصة ما سبق فإن القانون اليمني وإن لم يتضمن النص بصورة صريحة على تنظيم مسألة الاختصاص المكاني لمأموري الضبط القضائي والذي على ضوئه يستطيع المأمور أن يقوم بالبحث والتحري في جرائم المعلوماتية، إلا أنه من خلال النص سالف الذكر يتضح إمكانية تطبيقه على جرائم المعلوماتية مثلها مثل غيرها من الجرائم، وذلك في حالة قيام مأمور الضبط بإجراء التفتيش في حالة التلبس بالجريمة أو الندب على أن يتم التفتيش وفقا للقواعد التقليدية، أي دون أن يتطلب الأمر ترتيبات تقنية، ففي هذه الحالة فإن لمأمور الضبط القضائي تفتيش المتهم خارج نطاق اختصاصه في حالة أن ارتكبت الجريمة في نطاق اختصاصه، كتفتيش من يقوم بنشر صفحات تحتوي على مواد إباحية من مكان ما، ويتم استقبالها وفتحها في مكان أخر داخل الإقليم الوطني في الدولة. وسوف أرجئ إيضاحها بصوره أكثر تفصيلا إلى حين تناول مشكلة الاختصاص القضائي لعدم التكرار.

أماالقانون الجزائري، فقد نظم مسالة الإختصاص المكاني لمأموري الضبط القضائي بالنسبة لجرائم المعلوماتية، بحيث أوجد حلا لمشكلة الاختصاص المكاني في حالة أن ترتكب الجريمة في أكثر من نطاق اختصاص داخل الدولة، وذلك بالنص على امتداد إختصاص مأمور الضبط القضائي إلى كامل الاقليم في عدد من الجرائم منها جرائم المعلوماتية[1].

فبعد أن حدد المشرع الجزائري نطاق الاختصاص المكاني المحلي بنطاق الحدود التي يباشر مأمورو الضبط القضائي نشاطهم العادي، وتشمل كافة المنطقة السكنية

([1]) أدخل المشرع الجزائري عدد من التعديلات على نصوص قانون الإجراءات الجزائية من ضمنها تعديلات تتعلق بالاختصاص المكاني لمأموري الضبط القضائي – ضباط الشرطة القضائية- ضمن التعديل الأخير بالقانون رقم (06- 22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات، حيث مدد الاختصاص القضائي لمأموري الضبط القضائي في ملاحقة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات على مستوى الإقليم الوطني .

العمرانية التي يمارسون وظائفهم في إحداها، فقد وسع من ذلك الاختصاص ليشمل الاختصاص الوطني على امتداد كامل الوطن وذلك في حالتين:

الاولى: ترجع إلى الصفة الاصلية لمنتمي جهاز الضبطية القضائية بحيث وسع من الاختصاص الاقليمي بالنسبة لضباط الشرطة القضائية من مصالح الامن العسكري في البحث والتحري عن جميع الجرائم دون إستثناء[1].

والثانية: ترجع إلى طبيعة الجريمة، وذلك فيما يتعلق ببحث ومعاينة جرائم معينه منها جرائم المخدرات، والجرائم المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبيض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف [2].

ففي هذه الحالتين وسع المشرع الجزائري من اختصاص ضباط الشرطة القضائية ليشمل كامل الإقليم الوطني.

كما يمكن لضباط الشرطة القضائية، وتحت سلطاتهم أعوان الشرطة القضائية، أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب الجرائم المشار اليها، وكذلك مراقبة وجهة، أو نقل أشياء، أو أموال، أو متحصلات من ارتكاب هذه الجرائم، أو قد تستعمل في ارتكابها، وذلك مشروط بعدم اعترض وكيل الجمهورية المختص على القيام بذلك الإجراء[3].

ويتميز هذا الاختصاص المكاني الوطني بأنه اختصاص عام يشمل جميع ضباط الشرطة القضائية وأعوانهم مهما كانت الجهة التي يتبعونها سواءً أكانت الدرك الوطني أم الشرطة أم الأمن العسكري أم غيرها من الجهات التي نص عليها القانون، فيخول لهم القانون البحث والتحري والمعاينة بشأن عدد من الجرائم منها الجرائم الماسة بأنظمة

---

(1) راجع الفقرة (6) من المادة(16) إ.ج.ج رقم(06-22)المؤرخ في 20 ديسمبر2006 (ج.ر 84 ص4) .
(2)راجع: الفقرة (7) من المادة(16) إ.ج.ج.
(3) راجع: المادة (16مكرر) إ.ج.ج.

المعالجة الآلية للمعطيات، بعد أن كان النص يقتصر على تمديد الاختصاص بالنسبة لجرائم الارهاب والتخريب فقط [1].

وإضافة إلى الحالتين السابقتين اللتين بموجبهما يتم تمديد الاختصاص لمأموري الضبط القضائي والتي ترجع إحداهما إلى الصفة الوظيفية لمأمور الضبط، بينما ترجع الأخرى إلى طبيعة الجريمة، والتي منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فقد تم تمديد الاختصاص لمأموري الضبط في حالتين إضافيتين وبالامكان تطبيقهما ايضاً على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهاتان الحالتان هما حالة الاستعجال بدون طلب من السلطة القضائية - قاضي التحقيق- و حالة الاستعجال بطلب من السلطة القضائية، ففي الأولى يباشر مأمورو الضبط مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به، وفي الثانية يباشرون مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من قبل القاضي المختص قانونا، ويشترط في الحالتين إخبار وكيل الجمهورية الذين يباشرون مهمتهم في دائرة اختصاصه مسبقا.

وحالة الاستعجال قيدها بعض الفقهاء بحالة الضرورة التي يخشى إن تركت تسببت في ضياع الدليل، بينما يوسع جانب أخر في مدلولها ليشمل ضرورة البحث والتحري[2].

وإذا كان قانون الإجراءات الجزائية الجزائري قد حدد نطاق الإختصاص فجعله وطنيا بالنسبة لفئة من الضباط، وجعله اقليميا أو محليا بالنسبة لبقية اعضاءه الآخرين، فحدده بنطاق مباشرة عضو الضبطية القضائية لمهامه العادية كاصل، وامتداده إلى نطاق الحدود الاقليمية للمحكمة أو المجلس القضائي أو النطاق الاقليمي الوطني كإستثناء، فإنه لم يحدد ضوابط إنعقاد هذا الاختصاص، وعليه يجب العودة للقواعد العامة لتحديد هذا الإختصاص، وهذه الضوابط هي ذاتها التي اعتمدها القانون في تحديد نطاق اختصاص وكيل الجمهورية وقاضي التحقيق في المواد (37 و40)إ.ج.ج ويتحدد ذلك الاختصاص

(1) وقد تم تعديل تمديد الاختصاص وضم جرائم المساس بأنظمة المعالجة الآلية للمعطيات وجرائم أخرى إلى جرائم التخريب والإرهاب بموجب نص الفقرة(7) من القانون رقم (06-22)المؤرخ في 20 ديسمبر2006 (ج.ر 84 ص4) ، المُعدل للأمر رقم(95 -10)المؤرخ في 25 فبراير 1995(ج.ر 11، ص3) .

(2)راجع: عبد الله أوهايبية، مرجع سابق، ص212.

بإحدى إماكن ثلاثة هي إما مكان وقوع الجريمة، أو مكان إقامة المتهم، أو مكان القبض عليه فيه [1].

ونستخلص من ذلك بأن القانون الجزائري قد تميزعن القانون اليمني بمعالجة المشكلة المتعلقة بالاختصاص المكاني لممارسة مأموري الضبط القضائي لمهامهم، في متابعة وكشف الجرائم المعلوماتية التي نص عليها القانون الجزائري، داخل الاقليم الوطني، بحيث عالج مشكلة القيام بإجراء البحث والتحري خارج نطاق الاختصاص المكاني داخل الاقليم الوطني، حيث وأن متابعة وكشف جرائم المعلوماتية تحتاج إلى سرعة تنفيذ الإجراء قبل أن يقوم الجاني بمحو، أو تعديل، أو التلاعب بالبيانات، فجعل بإمكان مأموري الضبط القضائي- ضباط الشرطة القضائية- مواصلة البحث والتحري والمراقبة بإمتداد الاقليم الوطني في عدد من الجرائم منها جرائم المساس بأنظمة المعالجة الآلية للبيانات.

بينما عالج المشرع المشكلة في الجرائم التي تتعدى الاختصاص المكاني إلى خارج الجزائر أو ترتكب من الخارج عندما يتطلب الأمر الرقابة أوتفتيش أنظمة معلوماتية موجودة خارج الدولة عن طريق التعاون والمساعدة القضائية بين الجزائر والدول التي ترتكب فيها أو منها الجريمة، أو تتحقق فيها النتيجة كلها أو بعضها[2].

وعلى المشرع اليمني أن يحذو حذو المشرع الجزائري فيما يتعلق بهذه المسألة، بل إن عليه إضافة تعديلات متكاملة لقانون الاجراءات الجزائية بما يتناسب وتلك الجرائم، اتساقا مع الاتفاقيات والتوصيات الدولية في ظل النصوص الدستورية والقانونية المتعلقة بحماية الحقوق والحريات.

([1]) راجع المواد (37،و40) إ.ج.ج. لمزيد من التفصيل حول تحديد أماكن انعقاد الاختصاص لمأموري الضبط القضائي راجع: عبد الله أوهايبية، مرجع سابق، ص214.

([2]) لم يكتف المشرع الجزائري بالقواعد المنصوص عليها في القوانين التقليدية، والخاصة بتنظيم التعاون والمساعدة القضائية، بل عمل على استحداث نصوص قانونية تنظم التعاون الدولي والمساعدة القضائية بشأن جرائم المعلوماتية، وذلك في الفصل السادس من القانون رقم (09 - 04) المؤرخ في 5/ 2009/8 ويتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (ج.ر رقم 47، ص8).

المطلب الثالث

كشف وتجميع الأدلة

تعد مشكلة كشف وتجميع الأدلة غير المرئية والوصول إليها من أبرز المشكلات التي تواجه جهة التحري والاستدلال في سائر مجالات التخزين والمعالجة الآلية للبيانات، حيث تنتفي قدرة سلطة التحري من فحص البيانات المشتبه فيها بصورة مباشرة، خاصةً وأن اغلب التشريعات ومنها اليمني لم تتضمنصوصا قانونيةً تتضمن إجراءات تتناسب مع تجميع وكشف تلك الأدلة.

وتزداد المشكلة أو تتعقد بصورة أكثر من ذي قبل في حالة التلاعب بالبرامج، نظرا لتطلب الفحص الكامل للبرنامج، واكتشاف التعليمات غير المشروعة قدرا كبيرا من الوقت والجهد،بما لا يتناسب غالبا مع التكلفة الاقتصادية الكبيرة مقارنةً بحجم الجريمة[1].

فعملية تعقب الأدلة الإلكترونية –الرقمية- في أكثر من حاسوب وبأكثر من نظام داخل وخارج الحدود الإقليمية للدولة، وتجميعها والحفاظ عليها، من الإشكاليات التي تتعلق بمرحلة الاستدلال والتحقيق[2]، وهي أمور تستدعي القيام ببعض الأعمال الفنية،

([1]) وكمثال - من الواقع - لإعاقة الأدلة غير المرئية أثناء إجراءات التحري: قضية حدثت في ألمانيا الاتحادية عام 1971 وتتمثل وقائعها في سرقة أشرطة ممغنطة لشركة متخصصة في البريد تضم 300.000 من عناوين عملائها، وعند اكتشاف الشركة وجود تلك العناوين لدى شركة منافسة استطاعت أن تستصدر حكما بإعادة العناوين للشركة مالكتها، وبهذا الخصوص فقد سمحت الشركة لمساعد مأمور التنفيذ بالدخول إلى مقر الشركة ومركز الحاسب الآلي بها، وقد وجد كمّاً هائلاً من الأقراص لا يدري عنها شيئا ولا يعرف محتوياتها فما كان منه إلا أن قام بمغادرة مقر الشركة لما تشكل تلك الأدلة من صعوبة في تجميعها و استطلاعها، وقامت الشركة بعد ذلك ومن تلقاء نفسها بتسليم الأشرطة.راجع: هشام محمد فريد رستم، أصول التحقيق الجنائي الفني في الجرائم المعلوماتية، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون -جامعة الإمارات العربية المتحدة، في الفترة 1-2000/5/3م،ج2 ، ط3 ،2004 ، ص425.

[2] فمثلا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة. ومن البديهي أن تقف مشكلات الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم

وتستدعي تجهيز معامل جنائية متخصصة بجرائم الحاسب الآلي وجمع الأدلة الإلكترونية [1]. ويشترط في تلك الإجراءات الفنية أن لا تمس الحياة الخاصة للإفراد والحقوق المتعلقة بحرياتهم الشخصية .

ونتيجة للتطور التقني في مجال المعلوماتية وما ترتب عليه من استبدال أجهزة ووسائل الحفظ لتلك المعلومات من أوعية ورقية تقليدية إلى أوعية لا ورقية مستحثة، بسبب الزيادة الهائلة في كم المعلومات المخزنة، أو المعروضة، أو المنتجة، وما تبع ذلك في مجال الإجرام من استهداف لتلك المعلومات والأنظمة باستخدام أساليب ووسائل تقنية مستحدثة، استطاع من خلالها المجرم أن يخفي الآثار أو الأدلة، فقد وجدت العديد من الصعوبات التي تحول دون كشف وتجميع الأدلة[2].

المتصلة بالحاسب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود. راجع حسين بن سعيد سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، بحث منشور على شبكة الإنترنت، ص43.ص44، موقع المنشاوي، ت.د 2009/4/5 على الرابط.

http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014

(1) عائض بن فائز الشهري، صالح بن يحيى القحطاني، دور تقنية المعلومات في تعزيز الأمن الوطني وطرق حمايتها، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني الذي تم تنظيمه من قبل رأسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر 2007، مجلد 3، ص1276.

(2)ومن تلك الصعوبات التي تواجه سير الاستدلال وتتعلق بمشكلة كشف وتجميع الأدلة :

- **إخفاء الجريمة**: يستطيع الجاني إخفاء السلوك المكون للجريمة وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي في النبضات الكهرومغناطيسية التي تسجل البيانات عن طريقها، بحكم توافر المعرفة والخبرة الفنية في مجال الحاسبات وأنظمتها لديه، حيث بينت دراسة مسحية أجرتها لجنة تدقيق في مجال الإجرام المعلوماتي في المملكة المتحدة لعدد 6000 من المؤسسات التجارية وشركات القطاع الخاص، أن نصف حالات الاحتيال التي تتم بواسطة الحاسوب لم تكتشف إلا عن طريق المصادفة، ومن أشهر الأمثلة على ذلك ما حدث من (تيم كورادو) أشهر لصوص البطاقات الائتمانية على شبكة الإنترنت الذي لا يزال حراً طليقاً لأنه كلما اقتادته الشرطة إلى المحكمة كلما خرج دون أدانه، لعدم وجود دليل واحد ضده، فلقد قام هذا البريطاني باقتحام عشرات المواقع في شبكة الإنترنت واستولى على أرقام وبيانات ما يزيد على (124) ألف بطاقة ائتمانية تخص عملاء هذه المواقع، وقامبنشر أرقامها وبياناتها على شبكة الإنترنت، وقام أيضاً بإرسال بعض بيانات هذه البطاقات إلى بعض المواقع الشخصية لأفراد آخرين لا يعرفهم ولا يعرفونه، وقال (تيم كورادو) حين إلقاء القبض عليه للمرة الأولى، إن رهان رجال الشرطة ضده هو رهان خاسر، لأنهم لا يملكون دليلاً واحداً ضده، وقال أيضاً: إن هدف من قام بهذه العمليات التي يتهم بها هو إيقاظ الشركات التجارية التي يوجد لها مواقع على شبكة الإنترنت، ودفعها لإنجاز المزيد من إجراءات الحماية لمواقعها الإلكترونية، وبالتالي حماية أموال زبائنها، وأفلت (كورادو) من العقاب بسبب واحد وهو أن الموقع الذي تقول الشرطة انه استعمله في عملياته مسجل في شركة (Great solution) التي يوجد مقرها في مقاطعة ويلز البريطانية، ولكن كل البيانات الموجودة في هذا الموقع لا تدل أبداً على أي شيء يتعلق بشخصية تيم كورادو. راجع: عبد الله حسين علي محمود، مرجع سابق، ص345، وبخصوص تيم كورادو راجع: خالد الطويل: الجريمة الإلكترونية، مقال منشور على موقع شبكة روايات،ت.د 2009/11/16
http://www.rewayatnet.net/forum/archive/index.php/t-4004.html
- **التشفير الهادف إلى إعاقة الوصول إلى الدليل**: تشكل تقنية التشفير التي تستخدم من قبل المجرمين عقبة كبيرة أمام جهات التحري والتحقيق، حيث يصعب قراءتها وبالتالي الرقابة عليها ومتابعتها لمعرفة مضمونها، فتصبح المعلومات المهمة عرضة للتجسس عليها وتهريبها تحت غطاء التشفير، بالإضافة إلى أي بيانات تتعلق بجريمة معينة حيث يكون من الصعب على من يقوم بالتحريات مراقبتها ومعرفة ماهيتها كدليل على ارتكاب جريمة، إضافة إلى وجود قيود تتعلق بقانون الإجراءات الجزائية منها قصر إجراء التفتيش على النيابة مما يفوت الفرصة

ونتيجة لصعوبة كشف وتجميع الأدلة الإلكترونية التي يقابلها في الغالب نقص الخبرة والتدريب لأجهزة جمع الاستدلال، فهناك جرائم متعلقة بالحاسب الآلي وشبكة الإنترنت قد ارتكبت على مرأى ومسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم يد المساعدة لمرتكبي تلك الجرائم دون قصد، أو على سبيل واجبات المهنة التي يلزمهم بها هذا القانون أثناء محاولة كشف وتجميع الأدلة، مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، ونتيجة للمراقبة ومحاولة كشف وتجميع الأدلة بما تتسم به من صعوبات بجانب نقص الخبرة فقد تم إتلاف ما كان قد سلم من الملفات والبرامج[1].إضافة إلى صعوبات تتعلق بعمل مأمور الضبط بجانب نقص خبرته كمرشد جنائي عبر الإنترنت أو تكليفه من يقوم بذلك بهدف البحث عن الجرائم ومرتكبيها [2].

ومع أن هناك أقلية من الأفراد لديها مهارات التعامل مع تكنولوجيا المعلومات، غالبا ما توجد في البلدان ذات التطور التكنولوجي بشكل أكبر من البلدان الأخرى. إلا أن مثل هذا الأمر يجب أن ينتقل إلى الكل[3]، نظرا للتقنيات الجديدة المستعملة في كشف

على جهة التحري في ضبط الدليل إذا كان الوقت لا يكفي. راجع: عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب المصرية، القاهرة، 2004، ص48.

(1) راجع عبد الله حسين علي محمود، جريمة سرقة المعلوماتية، مرجع سابق، ص 355، وص354، وص355. وراجع ايضا: حسين بن سعيد بن سيف الغافري،الجهود الدولية في مواجهة جرائم الإنترنت، مرجع سابق،على الرابط .

www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014

(2) تقوم العديد من المؤسسات الضبطية حول العالم باستخدام نظام الإرشاد الجنائي عبر الإنترنت، من خلال الدفع بعناصرها وتجنيد الغير للدخول عبر العالم الافتراضي ، وبصفة خاصة عبر حلقات النقاش وقاعات البحث والاتصال المباشر، مستخدمين أسماء وصفات وهمية ومستعارة بقصد البحث عن الجرائم ومرتكبيها، وتقديم الجناة إلى المحاكمة، وبهذا الشأن فإن عضو الضبط القضائي يمكنه القيام بدور المرشد كما يمكنه تكليف من يقوم بذلك، وكل مافي الأمر هو الحصول على الإذن الذي يجب أن يشمل على رقم الحاسوب وصلاحيته للعمل وخلوه من العوائق التكنولوجية، واحتواؤه على برامج أصلية وليست منسوخة، وبالتالي فإن المرشد يستطيع الولوج إلى الإنترنت - بصفته شخصا عاديا- للبحث عن الجريمة والأدلة الموصلة إليها، فإذا ما ستطاع الحصول على معلومات تفيد في كشف الجريمة ومرتكبيها فإن عليه توصيل تلك المعلومات إلى جهة الضبط التي تقوم بدورها في تحديد مسار المجرم عن طريق برامج معلوماتية، والصعوبة في هذه المسألة تكمن في افتقار الجهات المشرفة على نظام الإرشاد الجنائي الإمكانيات التكنولوجية المتطورة، والمبرمجون الذين تكون مهمتهم تقصي الجريمة عبر الإنترنت والتعرف على مرتكبيها، إن لم توجد صعوبات أخرى تتعلق بالتشريع وعلى وجه الخصوص فيما يخص المراقبة البرمجية عبر الإنترنت والتي من خلالها يتم إرسال برمجية إلى خوادم مختلفة بقصد التوصل إلى مرتكبي الجرائم عن طريق الإنترنت مثل برمجية (Carnivore)، حيث لازال الإرشاد الجنائي عن طريق هذه البرامج محل خلاف لأنه يشكل عدونا على الحق في الخصوصية. راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص839، ص840.

(3) عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها(المراقبة الدولية للسياسة الجنائية) ملخص الترجمة العربية لمرشد الأمم المتحدة1999، ط1، دار النهضة العربية، القاهرة، 2005، ص115.

وتجميع الأدلة الالكترونية والتي تحتاج إلى تقنيين ومتخصصين للتعامل معها[1].

كما أن مشكلة كشف وتجميع الأدلة تتحقق من خلال الانتقال ومعاينة مسرح الجريمة، ومع أن معاينة مسرح الجريمة تعد من حيث الأصل عمل من أعمال التحقيق سيتم التعرض لها في حينه، إلا انه يشترط فيها حتى تكون من أعمال الاستدلال أن تكون في مكان عام وليس خاص[2]، فعلى الرغم من أن التعامل في مسرح الجريمة سواء أكان مسرحاً مادياً أم مسرحاً إلكترونياً يتطلب إجراءات روتينية معينة متفق عليها لحماية الدليل وإبراز قيمته الاستدلالية، إلا أن طرق حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة المادي عن مسرح الجريمة الإلكتروني أو الرقمي، ذلك أن التطبيقات أو البرامج والبيانات المرقمة يصبحان عنصران أساسيان يتحتم على أجهزة إنفاذ القانون وخبراء الأدلة الجنائية، جمعهما واستخلاصهما في مجال الجريمة المعلوماتية [3].

ومعاينة مسرح الجريمة في الجرائم المعلوماتية لا تتمتع في مجال كشف غموضها بنفس الدرجة في مجال الجريمة التقليدية، لأن الجريمة المعلوماتية قلما يترتب على ارتكابها آثار مادية، وفي حالة وجود آثار مادية، فغالبا ما تتعرض للإتلاف والعبث من قبل الأشخاص الذين يترددون على مكان أو مسرح الجريمة خلال الفترة التي تتوسط

---

(1) ومن تلك التقنيات المستخدمة في كشف وتجميع الأدلة : تقنية كشف واستعادة كلمة المرور، حيث ظهرت العديد من البرامج التي يتم من خلالها استعادة وكشف كلمة المرور، ويستفيد المحقق من هذه البرامج حتى يتمكن من الدخول إلى النظام أو الملفات المحمية لتفتيشها، وكذلك تقنية كشف وتجميع الأدلة والقرائن من رسائل البريد الإلكتروني، حيث تم تطوير برامج يتم بواسطتها البحث في ذاكرة الكمبيوتر عن الرسائل التي تم محوها والمعلومات المصاحبة لها وجعلها متاحة للمحققين والخبراء للاستفادة منها في كشف غموض الجريمة محل البحث، كذلك من التقنيات المستخدمة لكشف وتجميع الأدلة تقنية مراقبة البريد الإلكتروني بموجب برنامج= =يستطيع قراءة الرسائل التي قام صاحبها بمحوها، أو تلك التي لم يقم بتخزينها أساسا. لمزيد من التفصيل حول التقنيات الخاصة بتجميع وكشف الأدلة الإلكترونية راجع: مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2003

(2) تكون المعاينة لمسرح الجريمة من أعمال الاستدلال إذا كان مسرح الجريمة في مكان عام، وتكون من أعمال التحقيق إذا اقتضت المعاينة دخول مكان خاص أو له حرمة خاصة، فلا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد، وفي حالة مساسها بحقوق الأفراد فهي من أعمال التحقيق، وبالتالي يحظر على سلطة الاستدلال القيام بها، باستثناء أن يكون مأمور الضبط القضائي مخول بموجب القانون– جريمة مشهودة، أو انتداب - من جهة التحقيق للقيام بإجراءات - تفتيش أو ضبط- من شأنها كشف وتجميع الأدلة.راجع: أيمن عبد الحفيظ عبد الحميد سليمان، مرجع سابق، ص352، وراجع عفيفي كامل عفيفي ، مرجع سابق، ص 335، وراجع: محمد عادل، إجراءات جمع الأدلة في شبكة المعلومات،موقع كلية الحقوق جامعة المنصورة، ت.د 7/ 2008/8على الرابط:
http://www.f-law.net/law/showthread.php?t=1312

(3) ممدوح عبد الحميد عبد المطلب: استخدام بروتوكول IP/TCP في بحث و تحقيق جرائم الحاسوب، بحث منشور على شبكة ألنت، منتدى كلية الحقوق-جامعة المنصورة، تم التأكد من أن البحث مازال متاح على الشبكة في 2009/7/15على الرابط :

http://www.f-law.net/law/showthread.php?p=79241

ارتكابها واكتشافها(1).

وتتخذ المعاينة قواعد عدة بحسب نوعية الجريمة المرتكبة، فقد تستخدم طرق تقليدية كتصوير شاشة الحاسوب، وقد تتخذ طرق الكترونية، كتصوير شاشة الحاسوب باستخدام برامج معينة تسمى برامج التجميد، وقد تتخذ صورا أخرى كما في جرائم الملكية الفكرية بالتحفظ على صورة من النسخة، وطباعتها واستخراجها، وقد تتم عن طريق تتبع مسار الهكرة بإتباع الأسلوب الإرشادي الذي يحدد هوية الهاكر(2).

لذلك فإن معاينة مسرح الجريمة المعلوماتية يعد من الإشكاليات التي تعيق كشف الأدلة والوصول إليها، كونها تحتاج إلى مراعاة لقواعد وإرشادات فنية(3) قد لا يكون لدى مأموري الضبط القضائي الإلمام الكافي بها(4).

ونظرا لتلك الإشكاليات المتعلقة بكشف وتجميع الأدلة فقد عملت جهات لتطبيق

---

(1)عبد الله حسين علي محمود، جريمة السرقة في مجال المعلوماتية، مرجع سابق، ص365.

(2)عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص896.

(3) ومن تلك القواعد والإرشادات الفنية التي ينبغي مراعاتها من قبل مأموري الضبط القضائي أثناء معاينة مسرح الجريمة المعلوماتية هي:

- تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة وأخذ صورة لأجزائه الخلفية وسائر ملحقاته.
- ملاحظة طريقة إعداد نظام الكمبيوتر بعناية بالغة.
- وضع حراسة على كل جهاز حتى لايتم إتلاف المعلومات عن بعد أو عن طريق جهاز آخر في نفس المبنى.
- إثبات الحالة التي تكون عليها توصيلات وكابلات الكمبيوتر والمتصلة بمكونات النظام.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة
- التحفظ على معلومات سلة المهملات من الأوراق الملقاة والممزقة، وأوراق الكربون المستعملة، والشرائط والأقراص الممغنطة غير السليمة، وفحصها ورفع ما عليها من بصمات ذات علاقة بالجريمة.
- التحفظ على مستندات الإدخال والمخرجات الورقية لرفع ومضاهاة ما قد يوجد عليها من بصمات.
- قصر مباشرة المعاينة على المحققين ومن يخول لهم القانون القيام بإجراءات المعاينة، ممن تتوفر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات. لمزيد من التفصيل راجع عبد الله حسين علي محمود، جريمة السرقة في مجال المعلوماتية،مرجع سابق، ص366، وراجع أيضا وليد عكوم، التحقيق في جرائم الحاسوب، بحث منشور ،على شبكة الإنترنت، موقع القوانين العربية ، ت.د 2008/12/23، على الرابط:

http://www.arblaws.com/board/showthread.php?t=2280

وراجع أيضا:

Said Bachir, criminalité informatique en Algérie, état des lieux et perspectives, Mémoire Master université de Lausanne, suisse, 2009,idem. P.16 er 19.

وراجع محمد أبو العلا عقيده، التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، الخميس 2009/1/30 12،على الرابط :
http://www.arblaws.com/board/archive/index.php/t-2275.html

وراجع ايضا: محمد الأمين البشيري، مرجع سابق، ص.358.

(4) فنقص الخبرة التقنية في أوساط مأمور الضبط القضائي لازالت في الدول المتقدمة بالرغم من الجهود المبذولة في تخطي هذه المشكلة والمثال على ذلك، أنه في إحدى الدورات الأمنية القصيرة المنعقدة في كلية التدريب بأكاديمية الشرطة اليمنية في شهر نوفمبر 2008، في مجال تدريب كوادر من أجهزة الشرطة من قبل خبراء شرطة فرنسيين في مجال جرائم الحاسوب، طلب الخبير من أحد المتدربين عمل رقم سري خاص به حتى يتم إيضاح الطرق التي يستطاع من خلالها معرفة الرقم السري للدخول إلى جهاز الكمبيوتر-مسرح الجريمة- للتفتيش والعثور على الملفات التي تعين في كشف جريمة تزوير افتراضية، وبعد وضع كلمة السر حاول الخبير الدخول باستخدام أكثر من طريقة وبرنامج ولم يستطع الوصول إلى معرفة كلمة السر وتخطيها مبررا ذلك بأن الكلمة معقدة، فما كان منه إلا أن استخدام برنامج أخر يفتح الجهاز متعديا كلمة السر، فإذ كان هذا هو الحال في البلدان المتقدمة فكيف يكون الوضع في بلدان العالم الثالث والدول المتأخرة في متابعة تطور التكنولوجيا الرقمية.

القانون على عمل نماذج يتم من خلالها تحديد الخطوات الأساسية لكيفية تجميع الأدلة وفحصها، ومن ثم تحليلها وكتابة النتائج في تقرير [1].

وتثار مشكلة كشف وتجميع الأدلة من قبل رجال التحري والاستدلال في القانون اليمني كمشكلة تعيق إجراءات التحري والاستدلال في مجال الجريمة المعلوماتية، حيث لم يتضمن إجراءات مستحدثة يتم بواسطتها كشف وتجميع الأدلة المعلوماتية، بخلاف المشرع الجزائري حيث سمح بوضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، إذا استلزم الحال لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات[2].

وبالعودة إلى النصوص التقليدية في القانون اليمني يلاحظ بأنها قد تضمنت إجراءات يستدل من خلالها أن عمل مأمور الضبط القضائي في مجال التحري والاستدلال الهادف إلى كشف وتجميع الأدلة يقتصر على أعمال مادية صرفة، والتي منها إجراء المعاينة اللازمة، وضبط كل ما يتعلق بالجريمة، وبعبارة اشمل المحافظة على كل ما يتعلق بالجريمة، وسماع أقوال من يكون لديه معلومات عن الجريمة.

كما أن من تلك الإجراءات الانتقال إلى مكان الجريمة والذي من خلاله يمكن المحافظة على الآثار ورفعها، وضع الحراسة عليه لعدم السماح بالدخول إليه، وتصويره، وتحرير محضر جمع الاستدلالات[3] .

([1]) قامت وزارة العدل الأميركية بوضع نموذج حدد خطوات أساسية تشتمل على كيفية جمع الأدلة وفحصها وتحليلها، ومن ثم كتابة النتائج في تقرير، وهذا النموذج يوضح أنواع الأدلة، والمعلومات المستخلصة منها، وأماكن وجودها في الأجهزة وأنظمة المعلومات المختلفة، كما أنه يربط كل مجموعة من المعلومات بنوع محدد من جرائم المعلوماتية، فمثلا يحدد هذا النموذج قائمة بالأماكن المعتادة التي يمكن العثور على الملفات المخفية والملغاة فيها، وأيضا يحدد أنواع المعلومات الأخرى مثل الصور وكلمات السر وأرقام الهويات مثل رقم الضمان الاجتماعي، وهذه المعلومات بالذات مفيدة في التحري= =بأنواع محددة من جرائم المعلوماتية مثل التعدي على الهويات والصور الفاضحة، فالتعرف على أنواع المعلومات المفيدة وأماكن إخفائها في الأجهزة الرقمية المختلفة يعتبر خطوة ايجابية تساعد على تقديم أدلة قانونية يعتد بها عند تقديم الجناة للمحاكمة أمام القضاء..راجع .سلطان محيا الديحاني، مرجع سابق ، منشور على الشبكة على الرابط:
http://www.alqabas.com.kw/Final/NewspaperWebsite/NewspaperPublic/ArticlePage.aspx?ArticleID=230005

(2) راجع: المادة (3) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(3) وقد نصت على تلك الإجراءات التي تعد مادية المادة(91)إ.ج.ي حيث نصت على أن: (مأمورو الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها وفحص البلاغات والشكاوى وجمع الاستدلالات والمعلومات المتعلقة بها وإثباتها في

ومن خلال الإجراءات المشار إليها كأمثلة يلاحظ أنه يغلب عليها الطابع المادي وهي لا تصلح للاستدلال في مجال الجرائم المعلوماتية وتفصيل ذلك:

1. الانتقال إلى مكان الجريمة

يعد الانتقال إلى مكان الواقعة من أهم الإجراءات التي تسهل مهمة مأموري الضبط القضائي في كشف وتجميع الأدلة، والانتقال المقصود به في قانون الإجراءات اليمني والجزائري هو: الانتقال المادي الملموس، بخلاف الانتقال الذي يفترض في الجريمة المعلوماتية والذي هو عبارة عن انتقال معنوي، لا يستدعي سوى برامج معينة يستطيع بموجبها مأمور الضبط القضائي أن ينتقل معنويا ليفتش جهاز الحاسوب وهو يقبع في مكانه متى ما حصل على الإذن بذلك في حالة أن يتطلب الأمر ذلك، أو عندما تكون الجريمة في حالة تلبس، وذلك ما يثير التساؤل، هل يكتفى بالنص القانوني التقليدي الذي تم وضعه آنذاك وفي وقت لم يكن يتوقع ما سيؤول إليه العالم الرقمي من تطور، أم أن الحاجة تتطلب تعديل النصوص القانونية القائمة في قانوني الإجراءات اليمني والجزائري بما يلبي الحاجة الراهنة التي تتطلبها ظروف الحال لكشف وتجميع الأدلة المعلوماتية.

وبهذا الخصوص فقد رأى البعض بأنه لا يوجد ما يمنع من تقرير نص يمكن بمقتضاه السماح لمأمور الضبط بالانتقال عبر العالم الافتراضي خارج نطاق اختصاصه المكاني[1]، لأن القبول بهذا الإجراء وعدم القبول به لازال مسألة خلافية قد يترتب عليها قبول الإجراء أو بطلانه.

وقد سار المشرع الجزائري أخيراً على هذا النهج حيث تدارك هذه المشكلة من خلال نص المادة(5) من القانون رقم (09- 04) لسنة 2009 المتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، وذلك بتخويل

محاضرهم وإرسالها إلى النيابة العامة). وكذلك نصت المادة(92)إ.ج.ي على (إذا بلغ رجل الضبط القضائي أو علم بوقوع جريمة ذات طابع جسيم، أو من تلك التي يحددها النائب العام بقرار منه وجب عليه أن يخطر النيابة العامة،وأن ينتقل فوراً إلى محل الحادث للمحافظة عليه وضبط كل ما يتعلق بالجريمة، وإجراء المعاينة اللازمة وبصفة عامة أن يتخذ جميع الإجراءات للمحافظة على أدلة الجريمة وما يسهل تحقيقها، وله أن يسمع أقوال من يكون لديه معلومات عن الوقائع الجزائية ومرتكبيها، وأن يسأل المتهم عن ذلك، وعليه أثبات ذلك في محضر التحري وجمع الاستدلالات ويوقع عليها هو والشهود الذين سمعهم والخبراء الذين استعان بهم ولا يجوز له تحليف الشهود أو الخبراء اليمين إلا إذا خيف أن يستحيل فيما بعد سماع الشهادة بيمين، ويجب عليه تسليم تلك المحاضر لعضو النيابة العامة عند حضوره، وفي الجرائم الأخرى تحرر محاضر التحري وجمع الاستدلالات التي يقوم بها رجال الضبط القضائي طبقا لما تقدم وعليهم إرسالها إلى النيابة العامة للتصرف فيها). ويقابل النصوص السابقة في القانون الجزائري نص المادة(12) والمادة(42) إ.ج.ج .

([1]) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص832.

ضباط الشرطة القضائية الحق في تفتيش النظم المعلوماتية ولو عن بعد وفق الشروط المحدد بقانون الإجراءات الجزائية، حيث أن تفتيش النظم عن بعد لا يمكن أن يتم دون الانتقال الافتراضي .

ولما تم ذكره فليس هناك ما يمنع من أن يشمل نص القانون اليمني الخاص بالانتقال في مضمونه على الانتقال المعنوي إلى مكان الواقعة، بحيث يشيرا بصوره صريحة إلى ذلك بلفظ "سواءً أكان الانتقال مادي أو افتراضي بحسب ما تقتضيه المعاينة لمسرح الجريمة التي ارتكبت به الجريمة الجسيمة بالنسبة للقانون اليمني([1])، وكذلك إذا تم ارتكاب جناية في حالة تلبس في القانون الجزائري([2]).

2. وضع الحراسات اللازمة ورفع الآثار المعلوماتية

كذلك فإن من ضمن إجراءات التحري وضع الحراسات اللازمة للمحافظة على مسرح الجريمة حتى لا يتم التلاعب بالآثار قبل أن يتم رفعها.

فهل الحراسات التي تتطلبها الجريمة التقليدية تتساوى مع الحراسات التي تتطلبها الجريمة المعلوماتية، والتي هي في الأولى ذات طبيعة مادية، بينما في الثانية ذات طبيعة معنوية أو لامادية- برامج وبيانات-([3])، ناهيك عن ما تحتاجه الآثار التي تخلفت عن الجريمة من أدوات لرفعها؟

وهل الأدوات التي يتم بها رفع تلك الآثار ذات الطبيعة المادية تتساوى مع الأدوات اللازمة لرفع الآثار ذات الطبيعة المعنوية؟

وهل بإمكان مأمور الضبط الذي ليس لديه خبرة في الجانب التقني في مجال المعلوماتية القيام بتلك الإجراءات؟

بهذا الشأن يمكن القول بأن إجراءات وضع الحراسات اللازمة على مكان الواقعة- مسرح الجريمة - للمحافظة على الآثار حتى يتم رفعها لا يشكل صعوبة بالنسبة للجريمة

([1]) راجع: المادة (92) إ.ج.ي.
([2]) راجع: المادة (42) إ.ج.ج.
([3]) تستخدم في الوقت الحالي برامج وكيانات معنوية تقوم بما تقوم به الحراسات المادية في المحافظة على مسرح الجريمة، فبدلا من استخدام الحراسات التي تمنع التلاعب ومسح الآثار المادية من مسرح الجريمة، عن طريق وضع الحراسات المادية على ذلك المكان من قبل مأموري الضبط القضائي، فكذلك الحال عندما تكون الجريمة المرتكبة هي جريمة معلوماتية فإنه قد أصبح بالإمكان وضع الحراسات التي تتناسب مع نوع الجريمة، وتتمثل في كيانات معنوية وليست مادية تستخدم جوانب تقنية للمحافظة على مسرح الجريمة، مثل تقنية التجميد، حيث يقوم البرنامج المستخدم في المحافظة على مسرح الجريمة بتجميد البيانات المخزنة في النظام، ومنع أي دخول عليها من قبل المتهم أو الغير بقصد تغييرها بهدف تظليل جهة العدالة. راجع عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الحاسبب الآلي، مرجع سابق، ص871.

التقليدية، لأنها ذات طبيعة مادية والإجراءات المتخذة هي من ذات الطبيعة، فهي حراسة ذات كيان مادي تستطيع منع الدخول والخروج من وإلى مكان الواقعة، وهذا الإجراء منصوص عليه في القانونين اليمني والجزائري.

بخلاف الحراسات ذات الطبيعة المنطقية والتي تتمثل في البرامج والشفرات وما إلى ذلك من كيانات معنوية، يتم بواسطتها تامين مسرح الجريمة، ومنع الدخول أو التلاعب في البيانات أو الآثار ذات الطبيعة المعنوية الموجودة فيه، فهذا الإجراء لم يتضمنه قانون الإجراءات اليمني وكذلك الجزائري بصورة صريحة.

ومع ذلك فلم يقتصر القانون الجزائري على النص التقليدي في قانون الإجراءات الجزائية بخصوص وضع الحراسات على مسرح الجريمة، وإنما تضمن نصوصا مستحدثة في القانون رقم (09- 04) المتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، حيث أوجب في كل الأحوال على السلطة التي تقوم بالتفتيش أو الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وإذا استحال إجراء الحجز لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها[1].

وعلى المشرع اليمني عدم إغفال إضافة العبارات التي تتضمن إدراج الكيانات المنطقية التي تعد ضمن الوسائل الهامة التي تستخدم في المحافظة على الآثار المعلوماتية في مسرح الجريمة في أي تعديل قادم [2].

3. تحرير محضر جمع الاستدلال

([1]) راجع: المادتان (6، و7) من القانون رقم(09 - 04) مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما

([2]) ولقد شرعت النظم الإجرائية الحديثة، بقصد التوافق مع نظم تكنولوجيا المعلومات، إلى توسيع قاعدة الإرشاد الجنائي، في منطق البحث عن الجرائم ومرتكبيها لكي تشمل أحقية سلطة الضبط في الاتصال بمزود الإنترنت لكي يتولى التحفظ على السجلات المخزنة في الخادم المضيف، وكذلك ماهو متعلق بالاتصالات والأمور الأخرى، باستخدام برمجيات التجميد وغيرها من البرامج إلى حين استصدار إذن التفتيش ومن تلك التشريعات، التشريع الأمريكي وفقا لقانون الإجراءات 18 Us code see.2703 ، وكذلك قانون الإجراءات الفرنسي، حيث يجيز هذا الإجراء لسلطة التحقيق بموجب نص الفقرة(2) من المادة (31)، ولا تستثنى من الرقابة إلا المعلومات التي تدخل في نطاق سر المهنة المتواجدة في الأنظمة المعلوماتية بموجب نص المادة(60-1) من قانون الأمن الداخلي الذي عدل قانون الإجراءات الجزائية الفرنسي، وكذلك المعلومات التي تجمعها الكنائس أو أي تجمعات دينية، أو فلسفية، أو سياسية،أو نقابية وتتعلق باعضائها والمتراسلين معها، وذلك بموجب نص الفقرة(2) من المادة(31) من القانون رقم(17) لسنة 1978 الخاص بالمعلوماتية والحريات في فرنسا راجع شيماء عبد الغني محمد عطاء الله، الحماية الجنائية للتعاملات الإلكترونية، مرجع سابق، ص270.

من المشكلات المتعلقة بمرحلة جمع الاستدلال مشكلة تتعلق بتحرير محضر جمع الاستدلال، فيما إذا كان يتطلب القيام بهذا الإجراء عبر الإنترنت، حيث يمكن مع توافر إمكانيات البلاغ عبر الإنترنت وتقنيات التواصل في تحديد هوية الحاسب أو الخادم والمضيف والشبكات، والقيام بإجراءات التفتيش أو الحجز عن بعد، أن يقوم مأمور الضبط بتحرير محضر جمع الاستدلال عبر العالم الرقمي[1].فهل يمكن تطبيق النصوص التقليدية في القانونين اليمني والجزائري على محضر جمع الاستدلال.

وبهذا الخصوص لابد من استعراض النصوص القانونية في القانونين اليمني والجزائري، حيث تضمن القانون اليمني نصوصاً تتضمن ضرورة تحرير محضر جمع الاستدلال، وإرساله إلى النيابة، وذلك بعد أن أشار إلى الإجراءات التي يقوم بها مأمور الضبط القضائي في الجرائم الجسيمة، أو التي يحددها النائب العام بقرار منه، من الانتقال إلى مكان الواقعة، والتحفظ أو المحافظة على الآثار، وأخذ أقوال من كان متواجد في محل الجريمة، فقد أوجب على مأمور الضبط القضائي أن يدون كل ذلك في محضر جمع الاستدلال، ويرسله إلى النيابة العامة بقوله (وعليه أي- مأمور الضبط - أثبات ذلك في محضر التحري وجمع الاستدلالات والتوقيع عليها هو والشهود الذين سمعهم والخبراء الذين استعان بهم ولا يجوز له تحليف الشهود أو الخبراء اليمين إلا إذا خيف أن يستحيل فيما بعد سماع الشهادة بيمين، ويجب عليه تسليم تلك المحاضر لعضو النيابة العامة عند حضوره، وفي الجرائم الأخرى- غير لجسيمة- تحرر محاضر التحري وجمع الاستدلالات التي يقوم بها رجال الضبط القضائي طبقا لما تقدم وعليهم إرسالها إلى النيابة العامة للتصرف فيها[2].

وكذلك فقد تضمن القانون الجزائري النص على تحرير محضر جمع الاستدلال بقوله: (يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم، وأن يبادروا بغير تمهل إلى أخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم.

([1]) راجع عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص822.

(2) راجع الفقرة الثانية من المادة (92) إ.ج.ي رقم (13) لسنة 1994.

وعليهم بمجرد إنجاز أعمالهم أن يوافوه مباشرة بأصول المحاضر التي يحررونها مصحوبة بنسخة منها مؤشر عليها بأنها مطابقة لأصول تلك المحاضر التي حرروها وكذا بجميع المستندات والوثائق المتعلقة بها وكذلك الأشياء المضبوطة)[1].

ومن خلال النصوص السابقة يتضح بأن محضر جمع الاستدلال في القانون اليمني والقانون الجزائري يقتصر على المحضر التقليدي، الذي يتطلب لصحته تحريره والتوقيع عليه من قبل مأمور الضبط القضائي وكذلك الشهود والخبراء[2].

أما محضر الضبط الذي يتم تحريره عن طريق الإنترنت فغالبا ما يكون خاليا من التوقيع عليه من قبل الشهود والخبراء، ولذلك فلا بد من تحريره من الشروط التقليدية من خلال النص على ذلك في القانون، وذلك بالاكتفاء بالتوقيع الالكتروني على المحضر من قبيل مأمور الضبط القضائي فقط، ويكون التوقيع المطلوب في هذه الحالة أحد توقيعين إما توقيع الكتروني، أو توقيع يدوي عن طريق إخراج المحضر وتوقيعه وإعادة بالإسكان ومن ثم إرساله إلى جهة الاختصاص، على أن تحكم المسألة ضوابط فنيه تخضع للمناقشة أمام الجهات القضائية.

المطلب الرابع

تحديد هوية مرتكب الجريمة

لا تثير مسألة تحديد هوية المتهم في الجرائم التقليدية مشكلة مثلما هي في الجرائم المعلوماتية، ذلك أنَ الإجراءات التي يقوم بها مأمور الضبط القضائي في الجرائم التقليدية قد توصله إلى تحديد هوية مرتكب الجريمة، لأن تلك الإجراءات تتم من خلال وسط مادي ملموس، ويتحقق ذلك من خلال الأشخاص الذين كانوا في مكان الجريمة كشهود على الحادثة، أو الآثار التي يتركها الجاني، أو عن طريق التحريات التي تعتمد على الأوصاف وما إلى ذلك من أشياء مادية قد تقود في النهاية إلى تحديد هوية مرتكب

(1) الفقرة الأولى والثانية من المادة (18)، وكذلك المادة (40) إ.ج.ج .
(2) راجع المادة (92) إ.ج.ي رقم (13) لسنة 1994.

الجريمة، وذلك بخلاف الحال في الجرائم المعلوماتية التي يصعب في أغلب الأحوال الوصول إلى هوية مرتكب الجريمة.

وتعد مشكلة تحديد هوية مرتكب الجريمة المعلوماتية وعلى وجه الخصوص في جرائم الإنترنت من المشكلات التي تعترض أو تعيق إجراءات الاستدلال، ذلك أن المجرم قد يقوم بنشاطه الإجرامي من بلد غير البلد الذي يوجد فيه الكمبيوتر الذي بدأ انطلاق نشاطه منه، بحيث يتم تحديد نقطة الانطلاق من قبل أجهزة التحري في دولة معينة، إلا أن الحقيقة قد تبدو خلاف ذلك فقد يقوم المجرم بالتسلل إلى ذلك الجهاز بهدف إخفاء مكان التواجد الحقيقي لمكانه من خلال نقطة انطلاق وهمية، وبالتالي فإن عملية المراقبة في مجال المعلوماتية في مثل هذه الحالة قد تكون غير مجدية[1].

وتحديد هوية من قام بارتكاب جريمة معلوماتية يعتبر من إجراءات الاستدلال لكون مثل هذا الإجراء ليس فيه تعدي علي حقوق وحريات الأفراد، فليس له علاقة بالتفتيش أو الضبط، والغاية منه هو تحديد الجهاز الذي ارتكبت من خلاله الجريمة ومن ثم هوية مرتكبها، كعمل استدلالي يهدف إلى الكشف عن الجريمة ومرتكبها.

كما أن مسألة تحديد وتعيين المتهم في مرحلة البلاغ والاستدلال يعتبر من المهام الموكلة إلى مأمور الضبط القضائي أثر وصول البلاغ، وعليه فإنه في حالة وصول البلاغ فإن على مأمور الضبط القضائي تولي القيام بالتحريات اللازمة، واتخاذ إجراءات الاستدلال كاملة.

وتجدر الإشارة في هذا الخصوص إلى أن وسائل التقنية الحديثة في جرائم المعلوماتية قادرة على تحديد الأسلوب الذي ارتكبت من خلاله الجريمة، ويترك الأمر بعد ذلك لذكاء وفطنة مأمور الضبط القضائي لمعرفة المتهم، حيث يستطيع من خلال (IP) بروتوكول الإنترنت- تحديد الحاسوب الذي ارتكب من خلاله الفعل المجرم، غير أنه وأن أمكن التعرف على جهاز الحاسوب المرتكبة من خلاله الجريمة، فإن الوصول

([1]) قد يتعرف مركز الشكاوى الخاص بجرائم المعلوماتية في دولة معينة على هوية 100 ضحية، ويقرر أن النشاط الإجرامي صادرعن جهاز مقدم خدمات الكمبيوتر في كندا مثلا، ألا أن ذلك الجهاز قد يكون مجرد كمبيوتر تم التسلل إليه، لذلك فإنه من المفيد لمحللي مركز الشكاوى في الجرائم المعلوماتية أن يعرفوا المزيد عن نقطة الانطلاق الوهمية، فقد تكون هناك مجموعة في تكساس أو إفريقيا الغربية، أو رومانيا، تستخدم جهاز مقدم خدمات الإنترنت في كندا لجمع المعلومات عن الضحايا المحتملين. راجع دانيال لاركين، محاربة جرائم الإنترنت، مقال منشور على شبكة الإنترنت على موقع America -.gov ، ت .د 2009/11/13، على الرابط:
http://www.america.gov/st/democracy-arabic/2008/May/20081117124454snmassabla0.2601086.html

لمعرفة المتهم قد لا يكون بالأمر السهل، وذلك عندما يتم ارتكاب الجريمة من خلال محل انترنت أو أي مكان آخر، نظراً لاستخدام الإنترنت بشكل جماعي أو لفئات معينه، وبالتالي فإن البحث عن المتهم قد يتم من خلال الأوصاف التي يوصف بها المتهم من قبل الشخص الذي يدير المحل، بموجب تحديد وقت الدخول ومطابقته مع زمن حدوث الفعل أو الواقعة .

أما في حالة ما يكون الحاسوب يتبع شركة أو مؤسسة أو شخص كما في بعض الدول ومنها الولايات المتحدة الأمريكية التي تكون لأي مؤسسة أو شخص رقم (IP) خاص بذلك الشخص أو تلك المؤسسة، فإن بالإمكان الوصول إلى الشخص الذي كان يعمل على الحاسوب في وقت ارتكاب الجريمة [1].

ومن خلال ما سبق فإن مشكلة تحديد الهوية تكمن عندما لا يكون لمستخدم الإنترنت رقم(IP) خاص به كما في اغلب الدول ومنها العربية، بصوره اكبر من الحالة الثانية التي يكون فيها (IP) مخصصا لشخص معين أو مؤسسة كما في بعض البلدان، ففي هذه الحالة - الأخيرة- يكون بإمكان سلطة التحري والاستدلال تحديد مالك الجهاز، وسيكون هو المتهم بارتكاب الجريمة، إن لم يكن شخص آخر قد استغل عدم وجود مالك الجهاز وقام بارتكاب الجريمة، بمعنى أن إجراءات الاستدلال في هذه الحالة قد توصل إلى تحديد هوية مرتكب الجريمة، بينما تتعقد المسألة في الحالة الأولى - لعدم قدرة سلطة الضبط في الوصول إلى تحديد هوية مرتكب الجريمة، ذلك وأن أمكن تحديد الجهاز الذي ارتكبت منه الجريمة فمن الصعب تحديد هوية مرتكب الجريمة لكون رقم الـ (IP) يتغير بمجرد أن يتم فصل الخط عندما يتغير مستخدم آخر.

وإذا كانت مشكلة تحديد هوية الشخص مرتكب الجريمة مازالت آمرا حتميا في الدول المتقدمة التي لديها سلطة تحري واستدلال متخصصة في مجال مكافحة الجرائم المعلوماتية بالإضافة إلى قوانين -موضوعية وإجرائية- في ذات المجال. فكيف ستكون المشكلة بالنسبة للدول التي لازالت تفتقد لذلك[2] ؟.

(1)عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص834.

(2) ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (IP/TCP) في بحث و تحقيق جرائم الحاسوب، مرجع سابق على الرابط:

http://www.f-law.net/law/showthread.php?p=7924

وبالنسبة لموقف قانوني الإجراءات الجزائية اليمني والجزائري من تحديد هوية مرتكب الجريمة عبر الانترنت ونظم المعلوماتية فلم يتضمنا الإجراءات الفنية والتقنية المستحدثة التي يمكن أن يقوم بها مأمور الضبط القضائي لتحديد هوية مرتكب الجريمة المعلوماتية، إضافة إلى أن اليمن والجزائر من الدول التي لا يوجد فيها عنوان تحديد الهوية الذي يمتلكه أشخاص أو موسوسات(ip) مثل التي توجد في الدول المتقدمة، ولذلك فمشكلة تحديد الهوية تعتبر من المشكلات التي تعيق إجراءات الاستدلال والتحقيق في كلا البلدين، في حالة أن ترتكب جرائم معلوماتية تتطلب ذلك.

وبالعودة إلى النصوص التقليدية المتعلقة بكشف الجرائم والتحقق من مرتكبيها في مرحلة جمع الاستدلال يلاحظ بأن المشرع اليمني قد نص على ذلك ضمن المهام المناطة بمأموري الضبط القضائي في مرحلة جمع الاستدلال بقوله (مأموري الضبط القضائي مكلفون باستقصاء الجرائم وتعقب مرتكبيها) [1].

كما نص عليها القانون الجزائري بقوله (يجوز لضابط الشرطة القضائية منع أي شخص من مبارحة مكان الجريمة ريثما ينتهي من إجراء تحرياته، وعلى كل شخص يبدو له ضروريا في مجرى استدلالاته القضائية التعرف على هويته أو التحقق من شخصيته أن يمتثل له في كل ما يطلبه من إجراءات بهذا الخصوص)[2].

ومن خلال النصين سالفي الذكر يتضح بأنهما قد وضعا لتحديد هوية الشخص مرتكب الجريمة من خلال إجراءات مادية ملموسة، تتمثل في تعقب مرتكب الجريمة لمعرفة هويته، أو بمنع مغادرة مكان الحادث حتى يتم التحقق من هوية الموجودين في مكان الحادث، لكي يتمكن المأمور من الاستفادة في ذلك، إما بالوصول إلى هوية الجاني إذا كان لم يغادر مكان الحادثة قبل وصول المأمور، أو التعرف على الأشخاص الموجودين في مكان الجريمة للاستفادة من المعلومات التي يدلون بها في مجال الاستدلال والتحقيق في الوصول إلى هوية الجاني.

ومثل هذا لا يتحقق في مجال الجريمة المعلوماتية، حيث أن الجريمة مرتكبة في عالم افتراضي والتحقق من هوية مرتكبيها لا يتم إلا من خلال إجراءات فنية وتقنية، تتناسب مع طبيعة تلك الجريمة، لذلك كان لابد من الاعتراف بهذه الإجراءات وتضمينها

---

(1) المادة (92) من قانون الإجراءات الجزائية اليمني رقم (13)لسنة 1994.
(2) المادة (50) من الأمر رقم (66- 155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية.

في قانون الإجراءات الجزائية، أو النص عليها في قانون مستقل ، حتى يتسنى لمأمور الضبط القضائي التحقق من هوية الشخص من ناحية، ومن ناحية ثانية حتى يمكن الأخذ بذلك الإجراء في مجال الإثبات الجنائي وهو الإثبات عن طريق تحديد هوية الجاني عن طريق برتوكول الإنترنت (IP).

وقد تدارك ذلكالمشرع الجزائري أخيراً من خلال إصدارة قانونا مستقلا يتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث وضح بأن تحديد هوية الشخص يكون من خلال معرفة المعطيات المتعلقة بحركة السير، وعرفها أثناء توضيحه لبعض المصطلحات بأنها: معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة، كما تضمن القانون بعض الالتزامات على مقدمي الخدمات والمتعلقة بحفظ المعلومات المتعلقة بحركة السير، وجعل مدة الحفظ سنة كاملة بهدف تقديمها للسلطة المختصة في وقت الطلب [1].وبهذا الشأن فلابد من وجود شرطة قضائية متخصصة في مجال جمع الاستدلال في تلك الجرائم، لأن تشريع نصوص قانونية بدون تدريب أفراد للقيام بتلك الإجراءات سيصبح غير ذي جدوى.

المطلب الخامس

سلطات مأموري الضبط القضائي الاستثنائية

إلى جانب السلطات التي يقوم بها مأموري الضبط القضائي كسلطات أصلية تتمثل في أعمال التحري والاستدلال المشار إليها، فإن ثمة سلطات استثنائية تعد خروجا على الأصل، تمنح لمأموري الضبط القضائي وفقا للقانون وتعد من صميم أعمال التحقيق، أهمها ما يتعلق بالسلطات الممنوحة لمأموري الضبط القضائي في حالة التلبس بالجريمة (الجريمة المشهودة)، والتي من خلالها خول المشرع اليمني والجزائري لمأمور الضبط

(1) راجع: الفقرة (هـ) من المادة (2)، وكذلك المادة (11) من القانون رقم (09- 04) المؤرخ في 2009/8/5، يتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

القضائي القيام بإجراءات هي في الأساس من أعمال التحقيق، خروجا على القاعدة الأصلية التي تجعل مهام التحقيق من اختصاص النيابة العامة في القانون اليمني، وقاضي التحقيق، وقضاء الاتهام في القانون الجزائري، وذلك لأن وضوح التلبس من شأنه أن ينفي مظنة التعسف والخطأ من قبل مأموري الضبط القضائي[1]، ولما لأهمية سرعة اتخاذ الإجراء في حينه من أهمية في إثبات الجريمة وإدانة المتهم، كما توجد سلطات استثنائية في مجال الندب أو الإذن بالتفتيش أو الضبط، وتلك السلطات في مجال الجريمة المعلوماتية تعترضها بعض المشكلات.

1- الجريمة المشهودة في مجال المعلوماتية

سوف نتناول صور الجريمة المشهودة بإيجاز ومن ثم السلطات المخولة لمأمور الضبط القضائي حيالها لمعرفة مدى تحقق تلك الصور في الجريمة في مجال المعلوماتية، ومدى انطباق الإجراءات المتخذة بشأنها على الجريمة في مجال المعلوماتية:

أ- صور الجريمة المشهودة(المتلبس بها) وشروطها

تضمن قانون العقوبات اليمني الحالات التي تكون فيها الجريمة مشهودة، وحددها بأربع حالات هي[2]:

- مشاهدة الجريمة حال ارتكابها .
- مشاهدة الجريمة عقب ارتكابها ببرهة يسيرة.
- تتبع الجاني من قبل المجني عليه، أو العامة مع الصياح أثر وقوع الجريمة.
- مشاهدة أدلة الجريمة أو أثارها على المتهم بعد وقوعها بوقت قريب.

وأضاف المشرع الجزائري حالة أخرى إضافة إلى الحالات السابقة وهي اكتشاف الجريمة في مسكن والتبليغ عنها في الحال [3].

---

(1) عبد الله أوهايبية، مرجع سابق، ص224.

(2) نصت المادة (98) إ.ج.ي رقم(13)لسنة 1994 على حالات الجريمة المشهودة بقولها (تكون الجريمة مشهودة في حالة ارتكابها، أو عقب ارتكابها ببرهة يسيرة، وتعتبر كذلك إذا تبع المجني عليه مرتكبها، أو تبعته العامة بالصياح أثر وقوعها، أو إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملا آلات أو أسلحة أو أمتعه أو أشياء أخرى يستدل منها على أنه فاعلها أو شريك فيها، أو إذا وجدت به في الوقت المذكور أثر أو علامات تدل على ذلك).

(3) كذلك فقد نصت المادة(41)إ.ج المُعدَل والمُتَمم بالقانون رقم (06 - 22) المؤرخ في 20 ديسمبر 2006 على حالات التلبس بقولها (توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال، أو عقب ارتكابها، كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تتبعه العامة بالصياح، أو وجد في حيازته أشياء، أو وجدت أثار أو دلائل تدعو إلى افتراض

فتتحقق الجريمة المشهودة – المتلبس بها- إذا تحققت إحدى الصور السابقة، حيث تقوم الصورة الأولى على عنصر المشاهدة للجريمة من قبل مأمور الضبط القضائي حال ارتكابها في آي مرحلة من مراحل ارتكابها، وتثبت المشاهدة بالرؤية، أو السمع، أو الشم، وتقوم الحالة الثانية أيضا على عنصر المشاهدة، إلا أنها تقتصر على مشاهدة أثارها التي مازالت ظاهرة عقب ارتكابها، في حين أن الحالات الأخرى لا تقوم على حالة المشاهدة، بل إن القانون قد قرنها بضبط الجريمة في وضع معين يكون المشتبه في ارتكابها في حالة تقوم قرينة كافية على أنه ارتكب الجريمة، أو شارك فيها في وقت قريب من اكتشافها من خلال الآثار المتروكة على الجاني والأدلة التي تكون بحوزته، كما تعتبر كذلك في حال أن ارتكبت في منزل وبادر صاحب المنزل بالكشف عنها إذا كان الشخص المشتبه في ارتكابه لها في وقت قريب جدا من وقوع الجريمة[1].

ويشترط لتحقق الجريمة المشهودة،عدم التوسع في غير الصور التي أوردتها المادة (98)إ.ج.ي والمادة(41) إ.ج.ج كونها محددة على سبيل الحصر ولا يجوز القياس عليها.

كما يشترط أن يكون التلبس سابق على الإجراء لا لاحقا له، وأن يكون اكتشاف حالة التلبس قد تم بطريقة مشروعة، فمن يقوم بالنظر من ثقب الباب ويشاهد جريمة تقترف فإن الإجراء يكون باطلا.

ويشترط كذلك أن تثبت حالة التلبس بالنسبة لمأمور الضبط بالمشاهدة لها سواءً أكانت بصوره مباشره، أو بعد الانتقال إلى مكان الجريمة عقب الإبلاغ بها لمعاينتها ومعاينة آثارها [2].

وحول مدى تحقق صور الجريمة المشهودة في نطاق المعلوماتية فيرى البعض أن بالإمكان تحققها، في حال أن يكتشف مأمور الضبط القضائي أو المجني عليه الجاني أثناء

مساهمته في الجناية أو الجنحة، وتتسم بصفة التلبس كل جناية أو جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل وكشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء أحد ضباط الشرطة القضائية) انظر ج.ر 84 ص6.

(1)راجع: محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، مرجع سابق، ص85 وما بعدها، وراجع أيضا: عبد الله أوهايبية، مرجع سابق، ص227وما بعدها.

(2) ظاهري حسن، الوجيز في شرح قانون الإجراءات الجزائية، ط2، دار المحمدية العامة، الجزائر،1999،ص33، وص34.

قيامه باختراق شبكة، أو نظام معلوماتي، أو قاعدة بيانات تابع للمجني عليه، ويكون لديهما الإمكانية الفنية لمطاردة الجاني وتتبعه بقصد معرفته [1].

كما يمكن مشاهدة الجريمة حال حدوثها من خلال الانترنت إذا شاهد مأمور الضبط القضائي أو الغير الجريمة حال ارتكابها، وقد حدث ذلك في الواقع [2]، ففي مثل هذه الحالة تتحقق صورة الجريمة المشهودة بالمشاهدة عن بعد وعبر موجات كهرومغناطيسية، مثلها مثل المشاهدة المادية الملموسة التي نصت عليها القوانين التقليدية.

ويمكن أيضا أن تتحقق صورة مشاهدة المجني عليه بعد ارتكابه للجريمة ببرهة يسيرة في حال أن يقوم القائم على إحدى محلات الإنترنت، أثناء مراجعته للحاسوب عقب انتهاء العميل من استخدامه وقبل مغادرته المحل، باكتشاف ملفات تثير الاشتباه، وعند الإطلاع عليها يتبين أنها تحوي صور دعارة تم إنزالها أثناء عمل عضو الانترنت، مما يسمح بقيام حالة تلبس، ويترتب على ذلك عدم قيام حالة التلبس في حالة مغادرة الشخص مقهى الإنترنت ومن ثم الابتعاد عنه.

كذلك فإن مراقبة حاسوب عضو الإنترنت أثناء ظهور حركات مريبة منه واكتشاف قيامه بمحاولة اختراق أجهزة الغير تعد حالة تلبس [3].

ومع تطابق قيام حالة التلبس في الجريمة التقليدية في حال تتبع المجني عليه للجاني أو الغير عقب ارتكاب الجريمة مع الصياح كما ورد في القانونين اليمني والجزائري، إلا أن الصياح في جرائم المعلوماتية غير متصور حدوثه، لأن الملاحقة والتتبع اللتان تتم،

([1]) ومن ذلك قيام شركة (AOL) وهي شركة خدمات انترنت (ISP) بالولايات المتحدة الأمريكية باكتشاف أنشطة دعارة وترتيب لقاءات جنسية مع أطفال أثناء قيمها بمراقبة أنشطة المشتركين لديها، وعلى الفور قدمت أسماء المشتبه بهم للمباحث الفدرالية الأمريكية التي تمكنت من القبض على العشرات منهم بعد مراقبة أنشطتهم. راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت ، مرجع سابق، ص847.

([2]) أبلغ شخص، الشرطة الأميركية بجريمة قتل وقعت خلال "دردشة" له مع امرأة بالفيديو عبر الانترنت، وذكرت صحيفة "فيلادلفيا إنكوايارر أن الشخص شاهد جريمة قتل ميليني هاين (31 سنة) من منطقة ليبانون بولاية بنسيلفانيا خلال محادثته معها على الانترنت حيث قام على الفور بإبلاغ الشرطة بالجريمة، وقال مدير الشرطة في منطقة ليبانون، بولاية بنسيلفانيا، دانيال رايت إن هاين كانت تتحدث مع شخص على الانترنت عندما أطلق زوجها سكوت هاين (33 سنة) النار عليها من مسدسه وأرداها قتيلة، وأكد رايت أن الشخص الذي كانت يتحدث مع هاين على الانترنت اتصل بالشرطة لإبلاغها بالجريمة، وبعد الحادثة صعد الرجل إلى غرفة النوم في المنزل وانتحر بإطلاق النار على نفسه. وقد وردت القضية في أكثر من موقع منها مدونات البوابة، ت.د 2009/10/12 على الرابط:

http://blogs.albawaba.com/theoutsidersomali/67765/2009/10/12/189446-police-soccer-mom-video-chatting-when-shot

وراجع جريدة الرياض الصادرة يوم الاثنين الموافق 12/ أكتوبر 2009، على الرابط:

http://www.alriyadh.com/2009/10/12/article465633.html

([3]) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص848.

إنما هي إجراءات افتراضية، ومع ذلك فيوجد رأي بعدم اشتراط الصياح أثناء التتبع والملاحقة في الجريمة التقليدية، وذلك في حالة أن يكون المجني عليه أخرص، أو لا يستطيع الصياح لأي سبب كان [1].

وتعترض قيام حالة الجريمة المشهودة في مجال المعلوماتية بعض المشكلات منها، لزوم كشف حالة التلبس بالمشروعية، بمعنى أن الإجراء اللازم لكشف حالة التلبس يجب أن يكون مشروعا، وهذا يكون محل صعوبة في مجال الجريمة المعلوماتية نظرا لحداثتها وعدم وجود نصوص قانونية لتنظيمها، إضافة إلى تداخل القيام بالإجراء مع موضوع الحرية الشخصية التي يجب أن تكون مصانة بالقدر اللازم والضروري للحفاظ على حقوق الأفراد وحرياتهم، وبالتالي فيجب أن يكون الإجراء منصوصا عليه في القانون.

وفي هذه المسألة تثار مشكلة مشروعية التخفي عبر الإنترنت من قبل القائم بعمل التحريات، سواءً بهدف الكشف عن جريمة محددة حدثت، أم بغرض التوصل إلى البحث عن الجرائم ومرتكبيها بشكل عام، فغالبا ما يقوم عناصر من التحريات في بلد ما بالتخفي واتخاذ أسماء وهمية ومن ثم الولوج إلى الإنترنت والدخول إلى غرف المحادثات وحلقات النقاش، وتبادل الحديث مع الغير، بقصد التوصل إلى نتائج محددة تتمثل في التوصل إلى مرتكبي جرائم معينة، كما قد يتم التوصل إلى نتائج غير محددة، بهدف البحث عن الجرائم ومرتكبيها[2].

كما توجد مشكلة أخرى في حال حساب الزمن اللازم لقيام حالة التلبس والتي غالبا ما يترك أمر تحديدها لمأمور الضبط القضائي شريطة عدم تجاوزها مدة محددة، حيث والمدة بالنسبة للجريمة التقليدية قد قدرها البعض بساعات وفي الغالب بيوم أو يومين، والمهم أن لا يكون في تقدير الزمن إسراف[3]، بخلاف مدة التلبس في الجريمة المعلوماتية والتي يصعب تحديدها سيما إذا كان في الأمر مطاردة.

---

(1) إبراهيم حامد طنطاوي، التلبس بالجريمة وأثره على الحرية الشخصية،ط1، المكتبة القانونية، القاهرة، 1995، ص18، مشار إليه لدى عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص849.

(2) راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص850، ص851.

(3) محمد نجيب حسني، شرح قانون الإجراءات الجنائية المصري، ط2، دار النهضة العربية، القاهرة، 1988، ص543 مشار إليه لدى محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، مرجع سابق، ص93.

وقد عالج المشرع الجزائري مشكلة التخفي عن طرق الإنترنت بالنسبة لضباط الشرطة القضائية تحت اسم التسرب، وهو مصطلح أدق من مصطلح التخفي، حيث يتيح لضباط الشرطة القضائية أو أعوانهم تحت مسؤوليتهم بموجب إذن من وكيل الجمهورية أومن قاضي التحقيق بعد إشعار وكيل الجمهورية، إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في عدد من الجرائم منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات أن يقوموا بعملية التسرب وهي تعني: أخفاء ضابط الشرطة أو العون لشخصيته تحت أسم مستعار أو وهمي وظهوره بمظهر الفاعل أو المتعاون أو الشريك في اقتراف الجريمة بهدف المراقبة وصولا لكشف الجريمة وضبط المجرمين، وحدد مدتها بأربعة أشهر قابلة للتجديد، وعملية التسرب يمكن أن تتم من خلال الإنترنت لمراقبة المشتبه بارتكابهم جرائم معلوماتية والإيقاع بهم وفقا للشروط المشار إليها في القانون[1]، وعملية التسرب وفقا لما ذكر تتم بعد ارتكاب الجريمة، إلا أنه إذا شاهد ضابط الشرطة القضائية المكلف بالتسرب جريمة مشهودة أثناء قيامه بعملية التسرب فعليه القيام بالمهام المناطة به في الجرائم المشهودة.

ولحل مثل تلك الإشكاليات في القانون اليمني فيتعين إضافة صلاحيات لمأموري الضبط القضائي المتخصصين في مجال جمع الاستدلال والتحقيق في الجرائم المعلوماتية تتناسب مع تتبع الجريمة المشهودة عبر الإنترنت، مثل إقرار حالة التخفي والمداهمة لضبط الجريمة في حالة تلبس، بهدف المحافظة على الأدلة من المحو والتعديل[2] مع المحافظة على خصوصيات وحقوق الأفراد بالقدر اللازم.

ب- الإجراءات المخولة

وسع قانون الإجراءات الجزائية اليمني وقانون الإجراءات الجزائية الجزائري من صلاحيات مأموري الضبط القضائي في حالة التلبس بالجريمة، بحيث شملت إجراءات استدلالية وإجراءات أخرى هي من صلاحيات سلطات التحقيق، ومن تلك الإجراءات، الانتقال إلى مكان الواقعة لمعاينة الآثار المادية و المحافظة عليها، وسماع أقوال من كان

---

(1) راجع المواد (من 65 مكرر11 إلى 65 مكرر 18) من القانون رقم (06- 22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري. (ج.ر 84 ص8)

(2) يجيز القانون الأمريكي مداهمة أنظمة الحواسيب، بقصد البحث عن الجرائم دون الحاجة إلى التنبيه بذلك، باستخدام برمجيات معدة لهذا الشأن راجع: عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص851.

حاضرا أو من يمكن الحصول منه على إيضاحات، وضبط الفاعل واقتياده إلى اقرب ضابط شرطة قضائية، وضبط كل ما يؤدي إلى إظهار الحقيقة، وتفتيش شخص ومسكن المتهم بدون الحاجة إلى إذن في القانون اليمني، وبشرط إذن قضائي في القانون الجزائري[1]. ولأنه قد تم الإشارة إلى ما يتعلق بالمعاينة في مجال الجريمة المعلوماتية والانتقال المعلوماتي والقول بإمكانية القيام بتلك الإجراءات عبر الإنترنت، فسيتم الاقتصار في هذا الموضع على تناول تفتيش الحاسوب أثناء تفتيش منزل المتهم وكذلك تفتيش الحاسوب بموجب الضبط في حالة التلبس.

1) تفتيش نظم الحاسب الآلي في منزل المتهم

تضمن القانون اليمني النص على تفتيش منزل المتهم بناء على حالة التلبس دون الحاجة إلى إذن قضائي بذلك، حيث تنص المادة (101)إ.ج.ي (في الجرائم المشهودة المعاقب عليها بالحبس مدة تزيد على ستة أشهر يحق لمأمور الضبط القضائي القبض على كل شخص يستدل بالقرائن على أنه الفاعل للجريمة أو له علاقة بها إن كان حاضرا وأن يأمر بإحضاره إن كان غائبا)، وتنص المادة(102) بأن (لمأمور الضبط القضائي في الحالات المنصوص عليها في المادة السابقة أن يفتش المتهم ومنزله ويضبط الأشياء والأوراق التي تفيد في كشف الحقيقة متى وجدت أمارات قوية تدل على وجودها فيه)[2].

بخلاف القانون الجزائري الذي تطلب لتفتيش منزل المتهم إذن قضائي أو انتداب، حيث نصت المادة(44)من ق.إ.ج.ج رقم(06 -22)المؤرخ في 20 ديسمبر 2006

([1])راجع المواد (من 99-103)إ.ج.ي رقم (13) لسنة 1994 ،والمواد(42،و43،و44)إ.ج.ج. وبالنسبة لمواد القانون الجزائري فما زالت المادة (42) وفقا لما هي عليه في الأمر رقم (66- 155) المؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، تتضمن الصلاحيات الممنوحة لضباط الشرطة القضائية، بعد إبلاغ وكيل الجمهورية من الانتقال إلى مكان الجريمة، والمحافظة على الآثار، وضبط كل ما يؤدي إلى إظهار الحقيقة، أما المادة(43) فقد تم تعديلها بموجب القانون رقم(82-03) المؤرخ في 13فبراير 1982وتتضمن عقاب كل شخص لاصفه له يقوم بتغيير حالة الأماكن أو نزع الأشياء الموجودة في مكان الجريمة قبل الإجراءات الأولية للتحقيق القضائي، ويستثنى من ذلك إذا كان التغيير أو النزع للمحافظة على الصحة العامة أو السلامة، وتشدد العقوبة في حال أن يكون التغيير أو النزع من أجل عرقلة سير العدالة، والفارق بين هذا النص، والنص الأصلي قبل التعديل تكمن في زيادة عقوبة الغرامة. وكذلك المادة (44) فقد تم تعديلها بموجب القانون رقم(82-03) المؤرخ في 13فبراير 1982، ومن بعده القانون رقم (06- 22) المؤرخ 20 ديسمبر2006، حيث كانت تتضمن وفقا للنص الأصلي في الأمر رقم(66- 155) المؤرخ في 8 يونيو 1966 ، اسم مأمور الضبط القضائي بدلا من ضابط الشرطة القضائية وفقا للتعديلات الأخيرة، كما كانت تتيح للمأمور حق تفتيش منازل الأشخاص الذين ساهموا في ارتكاب الجريمة يدون تطلب الحصول على إذن قضائي، ولم تكن تتطرق للتفتيش في حالة التلبس ، أما النص وفقا لتعديل 1982، و2006، فقد تطلب شرط الإذن في تفتيش منازل الأشخاص الذين يظهر أنهم ساهموا في ارتكاب الجريمة أو أنهم يحوزوا وراقا أو أشياء لها علاقة بالجريمة من وكيل الجمهورية أو قاضي التحقيق، وزاد على ذلك نص المادة في تعديل 2006 أن أدخل التفتيش في حال التحري في الجريمة المتلبس بها أو التحقيق في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

([2]) المادتين (102،101) من قانون الإجراءات الجزائية اليمني رقم (13) لسنة 1994.

على (لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية، أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل، أو الشروع في التفتيش، ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها، أو التحقيق في إحدى الجرائم المذكورة في المادتين(37، 40)من هذا القانون[1].

ويكون المشرع الجزائري بذلك قد خالف القانون الفرنسي الذي غالبا ما يتسق معه في نصوصه القانونية، حيث نص القانون الفرنسي على جواز التفتيش في حالة التلبس بدون الحاجة إلى إذن في الفقرة الأولى من المادة(56) [2]، والتي مفادها بأنه في الجناية من النوع التي يمكن أثباتها بواسطة حجز أوراق أو مستندات أو أشياء تتعلق بالأفعال الإجرامية المرتكبة، فإن ضابط الشرطة القضائية ينتقل عاجلا إلى منزل أولئك الأشخاص لإجراء التفتيش وتحرير محضر بشأنه.

وعلى نفس السياق ذهبت قوانين أخرى إلى تفتيش مسكن المتهم في حالة التلبس بالجريمة [3].

([1]) المادة (44)من قانون الإجراءات الجزائية الجزائري رقم(06- 22)المؤرخ في 20 ديسمبر 2006(ج.ر84 ص6) والجرائم التي تضمنتها المادتين (37، و 40 هي جرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، وجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالصرف الصحي).

([2])**Article 56**

Ordonnance nº 60-529 du 4 juin 1960 art. 2 Journal Officiel du 8 juin 1960)
(Loi nº 99-515 du 23 juin 1999 art. 22 Journal Officiel du 24 juin 1999)
(Loi nº 2001-1168 du 11 décembre 2001 art. 18 Journal Officiel du 12 décembre 2001)
(Loi nº 2004-204 du 9 mars 2004 art. 79 I Journal Officiel du 10 mars 2004)
(Loi nº 2004-575 du 21 juin 2004 art. 41 Journal Officiel du 22 juin 2004)

Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal.

النص بالفرنسي من موقع قانوني يتضمن عدد من القوانين الجنائية والإجرائية لعدد من الدول، تم التأكد من أن القانون مازال منشور في الموقع بتاريخ 2009/8/17 ، على الرابط:

http://www.legislationonline.org/documents/section/criminal-codes

([3]) ومن تلك القوانين قانون الإجراءات الجنائية الايطالي من خلال نص المادة (224) حيث تضمنت النص على (أن لمأموري الضبط القضائي – في حالة التلبس – تفتيش الأشخاص وأي مكان يكون لديهم مبرر للاعتقاد بأن المتهم

وبناء على ما سبق يتضح بأن نص المادة (44)إ.ج.ج قد تضمنت تفتيش الحاسوب الآلي بصورة صريحة من خلال النص على خضوع جرائم المساس بأنظمة المعالجة الآلية للمعطيات لإجراءات التحري والتحقيق في حالة التلبس، وإن تطلبت شرط الإذن بذلك من وكيل الجمهورية أو قاضي التحقيق، وأكثر من ذلك فإن المشرع الجزائري قد نص على القواعد الخاصة بتفتيش نظم المعلوماتية والمعلومات المخزنة بتلك النظم، ويتضح من خللها في أن المشرع الجزائري قد أتاح لسلطة القضائية المختصة، أو لضباط الشرطة القضائية تفتيش نظم المعلوماتية في إطار قانون الإجراءات الجزائية، سواء كان ذلك التفتيش مرتبط بتفتيش منزل المتهم أم كان تفتيشا مستقلا بالحاسوب الآلي، وسواء كان تفتيش نظام المعلوماتية قد تم بصورة مباشرة أم عن بعد، ويشمل ذلك، التفتيش في حالة الجريمة المشهودة [1].

بخلاف نص المادتين (101 ،102) إ.ج.ي اللتين اقتصرتا على النص على تفتيش المتهم ومنزله، دون أن تشير إلى جرائم المعلوماتية أو جهاز الحاسوب، وإن لم تتطلب الحصول على إذن قضائي بذلك، وبذلك فإن نصوص القانون الجزائري أشمل من نصوص القانون اليمني من حيث تغطيته بوضوح للتفتيش عن جرائم المعلوماتية، ويكون نص القانون اليمني أفضل من حيث عدم تطلب الإذن في التفتيش في حالة التلبس، وكان الأولى الجمع بين الأمرين بتضمين النص اليمني التفتيش على جرائم المعلوماتية في حالة التلبس، وتضمين النص الجزائري ما يجعل صلاحية مأموري الضبط القضائي واسعة في مجال التفتيش على جرائم المعلوماتية، بحيث لا يتطلب الآمر إذن قضائي في حالة التلبس للمبررات السابق ذكرها.

وبذلك فإن نصوص القانون اليمني تقتصر على النص على إمكانية تفتيش الحاسب الآلي بموجب تفتيش منزل أو شخص المتهم في حالة التلبس، أي التفتيش المادي للمنزل أو الشخص، ومن ذلك أن توجد أثار ظاهرة على جهاز الحاسوب تفيد في الكشف عن الجريمة، أو أداة من الأدوات المستعملة في ارتكاب الجريمة تم إخفائها في تجويف

قد لجاء إليه أو أن به أشياء ينبغي ضبطها، أو آثارا يخشى عليها من العبث، غير أنه يجب على مأمور الضبط أن يبين في محضره السبب الذي حدا به لاتخاذ هذا الإجراء، وأن يرسل المحضر إلى سلطة التحقيق المختصة خلال 48 ساعة، وتصدق سلطة التحقيق على المحضر متى تبين لها صحته.راجع: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص159.

(1) راجع المادة (5) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الكيس- الإطار – الخارجي للحاسوب، أما التفتيش على البيانات المعالجة آليا، أو البرامج فالأحرى تضمينها ضمن النصوص القانونية القائمة أو النص عليها في قانون مستقل كما فعل المشرع الجزائري.

2) ضبط المتهم وتفتيش حاسوبه

كذلك فإن حالة التلبس تجيز الضبط والضبط يجيز التفتيش، فهل يمتد تفتيش الشخص إلى حاسوبه الشخصي؟

ولإيضاح ذلك على ضوء النصوص الإجرائية التقليدية، فقد تضمنت المادة (102) إ.ج.ي تخويل مأموري الضبط من ضبط المتهم في حالة الجريمة المشهودة، وتفتيشه إذا وجدت قرائن قوية تدل على أنه يخفي أشياء تفيد في كشف الحقيقة.

كما أوجب نص المادة(42) إ.ج.ج على ضابط الشرطة القضائية في حال الإبلاغ بجناية في حالة تلبس ضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة[1]، ففي مثل هذه الحالات التي يجيز فيها القانون ضبط المتهم و تفتيشه وفقا للقانون اليمني، أو ضبط كل ما يؤدي إلى إظهار الحقيقة وفقا للقانون الجزائري، فإنه يجوز تفتيش حاسوب المتهم، إذا كان في ذلك التفتيش فائدة في كشف الجريمة، شريطة أن يقتصر التفتيش وفقا لنصوص القانون اليمني على الأجزاء المادية للحاسوب وأنظمة المعلوماتية، لوضوح النص في ذلك.

أما بالنسبة للجوانب المنطقية في نظم المعلوماتية فنرى استحداث نصوص قانونية تتناسب مع حداثة الجريمة كما فعل المشرع الجزائري من خلال نصوص القانون رقم(09- 04) يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي سيتم إيضاحها أثناء التطرق لضبط أو حجز المعطيات المعالجة معلوماتيا عند تناول المشكلات المتعلقة بالتحقيق منعا للتكرار.

3) اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

كذلك فإن من الإجراءات التي تميز بها لقانون الجزائري عن اليمني في حالة التلبس بالجريمة أن أتاح لضباط الشرطة القضائية الحق في إعتراض المراسلات

([1]) راجع نصي المادتان (101،و102) من القانون اليمني رقم (13) لسنة1994 بشأن الإجراءات الجزائية، والمادة (42) من الأمر رقم (66 - 155) المؤرخ في 8 يونيو 1966يتضمن قانون الإجراءات الجزائية المعدل المتمم.

وتسجيل المحادثات والتقاط الصور[1]، بينما يظل هذا الإجراء في القانون اليمني من إختصاص النيابة العامة ومقتصرا على المراسلات والرقابة على المحادثات السلكية أو اللاسلكية لا الاعتراض[2] سوف يتم تناول مايخص القانون اليمني بشئ من التفصيل أثناء تناول الضبط لعدم التكرار بينما نتناول موقف القانون الجزائري في هذا الموضع لعلاقتة نصوصة بالمعلوماتية..

وبهذا الصدد فقد أجاز المشرع الجزائري لضباط الشرطة القضائية إذا اقتضت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات، أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أوجرائم تبييض الأموال والإرهاب، أو الجرائم المتعلقة بالتشريع الخاص بالصرف، أو جرائم الفساد بموجب إذن من وكيل الجمهورية القيام بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الإتصالات السلكية أو اللاسلكية.
- وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط أو تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة، أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

وقد أكد المشرع الجزائري على وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها إذا استلزم ذلك مقتضى حماية النظام العام أو التحريات في القضايا الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية [3].

ومع أن القانون قد أجاز أتخاذ هذه الإجراءات من قبل ضابط الشرطة القضائية إلا أن إتخاذ هذه الإجراءات يتطلب الحصول على إذن بذلك من وكيل الجمهورية، كما يقتصر إتخاذ تلك الإجراءات على حالة الضرورة في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، والجرائم

---

(1) راجع المواد (من 65 مكرر5 إلى 65 مكرر 10) من القانون رقم (06-22)المؤرخ في 20 ديسمبر2006 المُعدِل والمُتمِم لأمر رقم (66-155) المؤرخ في 8يونيو 1966 المتضمن قانون الإجراءات الجزائية

(2) راجع المواد (146، و148) إ.ج.ي.

(3) راجع: المادة (3) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال أو الجرائم المتعلقة بالصرف الصحي، وجرائم الفساد [1].

2- المشكلات المرتبطة بإذن التفتيش أو الإنابة القضائية

بالإضافة إلى المشكلات المتعلقة بالجريمة المشهودة والتي تم إيضاحها ضمن المشكلات المتعلقة بالسلطات الاستثنائية لمأموري الضبط القضائي توجد كذلك مشكلات إجرائية تتعلق بإذن التفتيش والإنابة القضائية التي تخولها السلطات القضائية لضباط الشرطة القضائية.

أ- وجوب الإذن القضائي

إذا كان المعمول به وفقا للقوانين الإجرائية في مجال الإجرام التقليدي تطلب الحصول على إذن قضائي من الجهة المخولة قانونا بإصداره، حتى يتمكن مأمور الضبط القضائي من القيام بإجرات معينة كالتفتيش أو الضبط، بموجب طلب يقدم من المأمور مبررا بدلائل وقرائن تستدعي القيام بالإجراءات المطلوبه [2]، فإنه من باب أولى لابد من سرعة صدور ذلك الإذن لمواجهة حالة الاستعجال التي تتطلبها سرعة أتخاذ الإجراءات الكفيلة بالحفاظ على الآثار والأدلة في مجال الاجرام المعلوماتي، نظرا لضالة الوقت اللازم لقيام المجرم بإخفائها والتلاعب فيها، ومن ثم جعل الجهود التي تبذل بعد ذلك من قبل مأموري الضبط القضائي تضيع هدرا، و تكمن المشكلة في حالة أن يكون الإذن لتفتيش نظام معين ويتطلب الأمر تفتيش نظام آخر مرتبط بالأول، بحيث تتيح الفترة التي يراد الحصول على إذن مكتوب بشأنها لتفتيش النظام الثاني إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها[3].

---

(1) راجع: المادة(65 مكرر 5) إ.ج.ج رقم (06-22)المؤرخ في 20 ديسمبر2006.

(2) تنص المادة(12) إ.ج.ي رقم (13)لسنة 1994على أن(1- للمساكن ودور العبادة ودور العلم حرمة فلا يجوز مراقبتها أو تفتيشها إلا بمقتضى أمر مسبب من النيابة العامة وفق ما جاء بهذا القانون، ويجب أن يكون ذلك بناء على اتهام سابق موجه إلى شخص يقيم في المكان المراد تفتيشية بارتكاب جريمة معاقب عليها بالحبس على الأقل أو باشتراكه في ارتكابها، أو إذا وجدت قرائن قوية تدل على أنه حائز لأشياء تتعلق بالجريمة، وفي جميع الأحوال يجب ان يكون أمر التفتيش مسببا. كما تنص المادة(44) من ق.إ.ج.ج رقم(06 -22)المؤرخ في 20 ديسمبر 2006 على (لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية، أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل ،أو الشروع في التفتيش.....)

(3) Jean-Wilfried noël, <<internet et enquête judiciaire>>, Le droit international de l'internet; Bruylant, 2002,p.245.

كما يثير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه، وتكمن المشكلة بصورة أكبر في حالة امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر منها الإذن، ودخوله في المجال الجغرافي لدولة أخرى، حيث ينتهك الامتداد سيادة الدولة الأخرى[1].

ويمكن ايضا أن تثارمشكلة أخرى فيما يتعلق بإذن التفتيش، وتتمثل في تحديد محل التفتيش، والأشياء التي يمكن أن يرد عليها بهدف ضبطها بطريقة تقنية ودقيقة، وبالتالي فإن الأمر يتطلب أن يكون القائم بالتفتيش لديه المعرفة والثقافة اللازمة في المجال الفني والتقني، وذلك ماتفتقده العديد من الدول من عدم وجود كوادر مدربة في هذا المجال، بخلاف الدول المتقدمة في مجال التكنولوجيا الرقمية حيث يمكن الاستفادة منها في الجوانب المتعلقة بالتحري والتحقيق في المجال المعلوماتي، وعلى سبيل المثال فيما يخص صيغة إذن التفتيش فيمكن الاستعانة بالمبادئ التي توصلت إليها الشرطة الكندية واستخلصتها من واقع الخبرة العملية، وتعني بتحديد محل التفتيش والأشياء التي يمكن أن يشملها في مجال الجرائم المعلوماتية[2].

ويكون على مأمور الضبط القضائي(ضابط الشرطة القضائية) طلب الإذن من الجهات القضائية كما لو كان المأمور في احدى حلقات النقاش وعلم بوقوع جريمة ما من أحد أعضاء الحلقة، أو ملاحظته أثناء مايكون على الشبكة لمواقع تقوم بإدارة شبكة دعارة أطفال، أو تحرش جنسي، أو صور مخله بالحياء، أو مواقع لترويج المخدرات، او غير ذلك من الجرائم التي ينص عليها القانون في البلد المعني.

([1]) محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، مقال على شبكة الإنترنت .مرجع سابق على الرابط:

http://www.arblaws.com/board/archive/index.php/t-2275.html

([2]) يشمل إذن التفتيش وفق النموذج الكندي البحث عن ضبط البرامج أو كيان الحاسب الآلي المنطقي، والتي تدخل فيها برامج التطبيق والتشغيل وما يتفرع عنهما، وكذلك البيانات المستخدمة بواسطة برنامج الحاسب الآلي أو كيانه المنطقي، كما يدخل ضمن إذن التفتيش السجلات المستخدمة في عملية الولوج في نظام المعالجة الآلية للبيانات، راجع عفيفي كامل عفيفي، مرجع سابق، ص347.

ومع ذلك فقد تم التخويل لجهات معينة بالقيام بتفتيش النظم المعلوماتية دون طلب استصدار إذن قضائي[1].

ومن أجل تخطي الصعوبات المشار إليها، فإنه يتعين أن لا يكون الإذن بالتفتيش محددا بمكان معين، بل يجب أن يمتد إلى تفتيش أي نظام آلي موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة، شرط عدم انتهاك سيادة دولة أخرى وان يحل قاضي التحقيق محل الشخص، صاحب المكان المراد تفتيشه بصورة مؤقتة.

كما يجب أن يتضمن إذن التفتيش الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[2].

ب- الإنابة القضائية

أجاز المشرع اليمني وكذلك الجزائري، تفويض مأموري الضبط القضائي بالقيام بأي عمل من أعمال التحقيق باستثناء الإستجواب حيث تنص المادة(116) إ.ج.ي على أن (يتولى النائب العام سلطة التحقيق والادعاء وكافة الاختصاصات التي ينص عليها القانون، وله أن يباشر سلطة التحقيق بنفسه أو بواسطة أحد أعضاء النيابة العامة أو من يندب لذلك من القضاة أو مأموري الضبط القضائي)[3].

وتنص الفقرة(6)من المادة (66) إ.ج.ج على (وإذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق، جاز له أن يندب ضباط الشرطة

(1) في الولايات المتحدة الامريكية وبالذات من بعد احداث 11 سبتمبر 2001 تم تخويل الجهات الاستخباراتية مثل المخابرات المركزية الامريكية (C I A) أوهيئة الأمن القومي الامريكي(N S A)الدخول إلى أي معلومات لتفتيشها عندما ترى ذلك، حتى لو كانت مخزنة في معالجات جهات امنية أخرى مثل ال (FBI)او جهات أخرى في مجال العالم الرقمي، وسوى كانت داخلة في اختصاصها ام لا دون الرجوع إلى أي جهة قضائية أو استصدار طلب قضائي بذلك.راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص823.

(2) قرار محكمة الجنايات منشور في مجلة العدل اللبنانية ،2000 ، ص 375، مشار إليه لدى وليد عكوم، مقال منشور على شبكة المعلومات الدولية،على الرابط :
http://www.arablawinfo.com/Researches_AR/126.doc

(3) المادة(116) إ.ج.ي رقم (13) لسنة1994(ج.ر19ج4 لسنة1994).

القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها في المواد من 138- 142)[1].

من خلال النصين سالفي الذكر يتضح أن الإنابة القضائية هي تفويض لمأمور الضبط القضائي للقيام بإجراء واحد أو بعض إجراءات التحقيق الابتدائي ما عدا الاستجواب و المواجهة [2].

و لكي تكون الإجراءات المتخذة بموجب الإنابة، أو الندب صحيحة فلابد من تحقق مجموعة من الشروط أهمها:

1) أن تكون صادرة من سلطة مختصة بالتحقيق تتمثل في عضو النيابة العامة في القانون اليمني، وقاضي التحقيق في القانون الجزائري، وأن تكون السلطة مختصة نوعيا و إقليميا و أن تكون مكتوبة و موقعة من طرفه[3].
2) أن يصدر عضو النيابة أو قاضي التحقيق الإنابة القضائية لأحد مأموري الضبط القضائي، وبالتالي فلا يجوز ندب معاونيهم أو مساعديهم، والخلاف في هذه المسألة بين القانون اليمني والجزائري، تتمثل في أن قاضي التحقيق في القانون الجزائري له أن ينيب ضابط شرطة قضائية، أو قاضي أخر في نفس المحكمة، بخلاف اليمني الذي يقتصر حالة الندب على مأمور الضبط القضائي، عدا حالة أن تكون الإنابة إلى خارج اختصاص عضو النيابة، فله أن يكلف عضو النيابة المختص، وللعضو الأخر أن يقوم بالعمل بنفسه وله أن ينتدب أحد مساعديه، أو مأمور ضبط قضائي[4]، وقد تضمن حكم الفقرة الأخيرة أيضا القانون الجزائري[5].

([1])الفقرة(6) من المادة(68)من الأمر رقم (66-155)المؤرخ في 8 يونيو 1966 المعدل والمتمم بعدد من الأوامر والقوانين أخرها القانون رقم (06-22)المؤرخ في20ديسمبر2006.

([2]) الفقرة(2) من المادة (139) من القانون رقم (82-30) المؤرخ في 18 غشت 1982 المعدل والمتمم للأمر رقم(66-155) المؤرخ في 8يونيو 1966 يتضمن قانون الإجراءات الجزائية، والمادة (117) من القانون رقم (13) لسنة 1994 بشأن قانون الإجراءات الجزائية.

([3])وتكون الجهة المختصة بالتحقيق هي النيابة العامة في القانون اليمني وقاضي التحقيق في القانون الجزائري وفقا لنص المادة (115) إ.ج.ي والمادة (3/38) إ.ج.ج التي تبين أن قاضي التحقيق هو صاحب الاختصاص في التحقيق الجنائي، والمادتين (67،و 73) إ.ج.ج حيث توضحان الشروط التي بموجبهما يتم فتح التحقيق. لمزيد من التفصيل راجع محمد راجح نجاد، مرجع سابق، ص184 وما بعدها، وعبد الله أوهايبية، مرجع سابق ص273 وما بعدها.

([4])راجع المادة(138)من الأمر رقم (66-155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية، والمادة(117)إ.ج.ي.

([5])راجع المادة (142)إ.ج.ج.

3) أن تكون الإنابة محددة بعمل أو أكثر من أعمال التحقيق فلا يجوز للمحقق ندب مأموري الضبط القضائي للتحقيق بقضية بأكملها[1].

4) لا يجوز ندب مأمور الضبط القضائي لاستجواب المتهم و المواجهة و سماع المدعي المدني، وبهذا الشأن فقد استثنى المشرع اليمني استجواب المتهم في حالة الندب عند الضرورة الذي يخشى معها فوات الوقت متى كان ذلك لازما لكشف الحقيقة[2]، بخلاف المشرع الجزائري الذي جعل إجراء الاستجواب مقتصرا على سلطة التحقيق[3].

5) لابد أن يشمل أمر الندب أو الإنابة على بيانات توضح مصدر الأمر، و صفته، و توقيعه، و من صدر له الأمر، و الأعمال المراد تحقيقها و اتخاذها، و نوع الجريمة موضوع المتابعة و تاريخ الأمر.

6) أن يلتزم مأمور الضبط القضائي - ضابط الشرطة القضائية- بتحرير محضرا بشأن ما قام به من إجراءات يحرره كاتب يصطحبه معه من المعينين لذلك، أو يكلف من يقوم بكتابة المحضر في حالة عدم وجود كاتب معين لذلك، ويحرره بنفسه في حالة الضرورة، ويوافي به جهة الاختصاص خلال المدة التي يحددها عضو النيابة أو قاضي التحقيق، أو المدة التي يحددها القانون في حالة عدم تحديدها من قبل المختص بالندب [4].

ولتطبيق حالات الندب وشروطه في مجال الجريمة المعلوماتية، يلاحظ بأنه لا يوجد ما يمنع من تطبيق النصوص الخاصة بالندب، أو الإنابة في القانون اليمني والقانون الجزائري وفقا لما تم التنويه اليه، شريطة أن تكون إجراءات التحقيق التي يتم الندب بها أو الإنابة يمكن القيام بها من قبل مأموري الضبط القضائي، حيث أن فاقد

([1])راجع المادة(139) من القانون رقم(82-03)المؤرخ في 18اغسطس 1982(ج.ر 7،ص309) المعدل والمتمم لقانون الإجراءات.

([2]) المادة (118)إ.ج.ي.

([3]) راجع المادة(117)من القانون اليمني رقم(13)لسنة 1994 بشأن الإجراءات الجزائية، والمادة (139)إ.ج.ج رقم (82-03)المؤرخ في 18 أغسطس 1982(ج.ر7ص309)، وتشمل نفس مضمون المادة قبل التعديل – في ظل الأمر رقم (66-155) المؤرخ في 8يونيو 1966 يتضمن قانون الإجراءات الجزائية- باستثناء تغير مسمى مأموري الضبط القضائي بضباط الشرطة القضائية، وعدم منح صلاحية مأمور الضبط –ضابط الشرطة القضائية الحق في استجواب المتهم مطلقا وفقا لقانون 1982 ، بخلاف النص قبل التعديل الذي حضر الاستجواب على مأمور الضبط إلا إذا طلب المتهم ذلك

([4]) انظر المادة (119) إ.ج.ي، وكذلك الفقرة الأخيرة من المادة (141) إ.ج.ج.

الشيء لا يعطيه[1]، فأنى لمأموري الضبط القضائي الغير مدربين في مجال مواجهة جرائم المعلوماتية، أن يقوموا بإجراءات تتطلب أن يكون القائم بها لدية إلمام بالجوانب التقنية والفنية، وأكثر من ذلك فإن سلطة التحقيق نفسها قد تكون غير مختصة في مجال التحقيق في جرائم المعلوماتية، وتقوم بانتداب مأموري ضبط غير متخصصين، وبذلك تكون مشكلة المواجهة لتلك الجرائم أكبر مما هي عليه.

فيشترط في مأمور الضبط القضائي في مجال تفتيش نظم الحاسوب والإنترنت أن يكون ذا خبرة في مجال تفتيش نظم الحاسوب والشبكات، يستطيع التعامل مع مخرجات الحاسوب والإنترنت، ومع الأقراص والشرائط الممغنطة، بهدف الحفاظ على أدلة جرائم المعلوماتية، وأن يتم تدريب شرطة متخصصة في هذا المجال، إضافة إلى قبول دفع من خريجي كليات الحاسوب والبرمجيات، في كلية الشرطة وتخريجهم ضباط مؤهلين في هذا المجال [2].

كما أنه لا يمنع في مجال التفتيش على نظم الحاسوب وشبكة الإنترنت، في أن يكون أمر الندب أو الإنابة مكتوباً، إلا أن تبليغه في مجال هذه الجرائم تحقيقا للسرعة قد يتم عن طريق الفكس أو الإنترنت ويتم التفتيش بموجبه إلا أن يتم إرسال النسخة الأصلية[3].

([1]) وكمثال على عدم وجود سلطات متخصصة في مجال التحقيق في جرائم المعلوماتية، عندما أردت التحقق والاستفادة من الإجراءات المتخذة بشأن قضية منظورة لدى النيابة الجزائية المتخصصة، تتمثل في اتهام أشخاص بقضايا التجسس لصالح إسرائيل عن طريق البريد الإلكتروني، إلا أنني لم أجد الإجابة الفنية ذات الطابع التقني لدى سلطة التحقيق، وما قيل هو أن إجراءات التفتيش على البريد الالكتروني وكل ما يتعلق بالأمور التقنية قامت بها الإدارة العامة لمكافحة الإرهاب، وبسبب ضعف الإجراءات فقد تم الاستعانة فيما بعد بخبيرين من وزارة المواصلات، وبعد الذهاب إلى المحكمة مرة أخرى لمعرفة الإجراءات التقنية المتخذة والحصول على نسخه من الحكم الابتدائي، لم أتمكن من ذلك بسبب أن القضية مازالت في محكمة الاستئناف حسب إفادة رئيس النيابة الجزائية المتخصصة، وفي زيارة سابقة لإدارة مكافحة الإرهاب ومقابلة المدير العام يوم الثلاثاء 2006/4/17 في قضية أخرى تبين أن الإجراءات المتخذة بشأنها هي إجراءات تقليدية وليدة الصدفة ليس إلا، استطاعوا من خلالها أن يتوصلوا إلى اعترافات للمتهمين بتحويل أكثر من ثلاثة ملايين دولار من حساب مالي لشركة نفطية متواجدة في اليمن من رصيدها في بنك في أمريكا، وتم التحويل إلى ماليزيا ومنها إلى اليمن.

(2) ونظرا لأهمية التخصص في مجال التحري والتحقيق في الجرائم المعلوماتية، وكذلك في مجال العمل الفني والخبرة، فيتم التأهيل عبر أكثر من برنامج منها: برنامج دبلوم سنتين للتحري لتأهيل فني حاسب جنائي للتدريب على الأدوات المستخدمة في التحري الرقمي، وبرامج البكالوريوس في الحاسب الجنائي في تخصصات مختلفة وكذلك الماجستير، إضافة إلى الدورات التخصصية المختلفة مثل محلل بيانات، ومحقق في مجال جرائم الحاسب، راجع: هند بنت سليمان الخليفة، الحاسب الجنائي في الدول الغربية دورة استطلاعية، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني، الذي تم تنظيمه من قبل رياسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر ،2007، المجلد2، من ص1022: ص1024.

([3]) علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، ط1، عالم الكتاب الحديث، اربد –الأردن، 2004، ص110.

فالإنابة للتفتيش في جرائم المعلوماتية تحتاج إلى سرعة، وبالمقابل فقد يكون الشخص الذي يتم إنابته في مكان غير المكان الذي يتواجد فيه قاضي التحقيق أو وكيل الجمهورية، وبالتالي فيمكن في مثل هذه الحالات إرسال نسخة من أمر الإنابة عن طريق الانترنت، بالبريد الالكتروني مثلا واعتبارها بمثابة النسخة الأصلية، ومثل هذا يتفق مع من يرى بأن الإنابة يمكن أن يتم إرسالها إلى جهات مماثلة من التراب الوطني بالوسائل الحديثة في حالة أن تتطلب الضرورة ذلك، مثل الفاكس والتلكس،على أن يتم توضيح البيانات الجوهرية والتي منها نوع التهمة واسم وصفة القاضي المنيب[1].

والخلاصة تكمن في أن القانون اليمني لم يتضمن قواعد التفتيش والضبط المتعلقة بجرائم المعلوماتية، والتي تخول لمأموري الضبط القضائي في الحالات الاستثنائية استخدام التقنيات اللازمة للتفتيش والضبط في نظم المعلوماتية ولو عن بعد، وما زالت النصوص التقليدية هي المعمول بها مع القصور التي تكتنفها، بحيث لا يمكن إعمالها في قضية التفتيش عن بعد، أو التفتيش الافتراضي عن طريق الإنترنت، وكذلك الضبط وحجز المعطيات المعلوماتية.

بخلاف القانون الجزائري الذي عالج المسألة من خلال التعديلات التي تمت في قانون الإجراءات الجزائية 2006، وكذلك من خلال القانون رقم (09- 04) لسنة 2009 الذي تضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها، والذين من خلالهما يمكن للسلطات المختصة أصلية كانت أو استثنائية القيام بإجراءات التفتيش أو الضبط في نطاق المعلوماتية.

([1]) أحسن بوسقيعة، التحقيق القضائي على ضوء قانون 26 يونيو 2001، ط2، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص112.

المبحث الثاني

مرحـــلـــــــة التحـقـيـق

التحقيق الابتدائي هو: نشاط إجرائي تقوم به سلطة قضائية مختصة للتحقيق في مدى صحة الإتهام الموجه بشأن واقعة جنائية معروضة عليها[1].

وهو: مرحله لاحقة لإجراءات جمع الاستدلال، أو البحث التمهيدي الذي يقوم به مأموري الضبط القضائي، وسابقة لمرحلة المحاكمة التي تقوم بها جهة الحكم.

ومرحلة التحقيق في القانون اليمني تقوم على درجة واحدة تختص بها النيابة العامة، كما أن القانون اليمني يجمع بين سلطة المتابعة والاتهام وبين نظام التحقيق ويجعل تلك المهام من اختصاص النيابة العامة مثله مثل النظام الإجرائي المصري، والأنظمة التي تجمع بين التحقيق والاتهام توصف بأنها الأشد خطرا من بين الأنظمة على الحقوق والحريات الفردية[2].

أما القانون الإجرائي الجزائري فقد جعل التحقيق على درجتين الأولى بواسطة قاضي التحقيق وفقا لنصوص المواد(66: 175إ.ج.ج)، والثانية بواسطة غرفة الاتهام كدرجة عليا للتحقيق وفقا لنصوص المواد (176: 211إ.ج.ج)، كما أنه يفصل بين التحقيق والاتهام والمتابعة بهدف تحيق ضمانات كافية للحقوق والحريات الفردية، وذلك هو المتبع في أغلب الأنظمة الإجرائية الحديثة، لأن جمع السلطتين في جهة واحدة فيه خطر على الحقوق والحريات، إذ يصعب على القاضي الوقوف موقف المحايد لاجتماع صفتي الخصم والحكم في جهة واحدة، وبالتالي فإن المشرع الجزائري قد خول سلطة المتابعة والاتهام لجهاز النيابة العامة ممثلة بالنائب العام ومساعديه على مستوى كل مجلس قضائي طبقا للمادة(29أ.ج.ج)، وخول سلطة التحقيق لجهة تحقيق مستقلة ومحايدة لا تخضع لغير القانون.

---

(1) عبد الله أوهايبية، مرجع سابق، ص308.

(2) راجع: محمود محمود مصطفى، تطور قانون الإجراءات الجنائية، بند86، ص87. مشار إليه في مؤلف عبد الله أوهايبية، المرجع سابق، ص309.

وتختلف مرحلة التحقيق عن مرحلة جمع الاستدلال في أن مرحلة التحقيق تعد أشد خطورة من الاستدلال، لأنها قد تمس حقوق وحريات الأفراد، وقد تتسبب في الاعتداء على خصوصياتهم في إطار الموازنة القائمة بين المحافظة على حق الفرد في الخصوصية، وحق المجتمع في ملاحقة الجاني وعقابه.

وتعد إجراءات التفتيش، والضبط، ومراقبة الاتصالات وسماعها، والاطلاع على الرسائل من أهم إجراءات التحقيق، لذلك فقد تضمنت القوانين نصوصا قانونيةً تنطوي في إطارها على ضمانات تهدف إلى المحافظة على حقوق الأفراد وعدم المساس بها إلا في أضيق الحدود، وتتمثل تلك الضمانات، في ضمانات ترتبط بالإجراء المتخذ مثل تحديد الغاية من التفتيش، وعدم فتح الأوراق المغلقة، والنوع الآخر من الضمانات يتمثل في القائمين على هذه المرحلة بأنهم ليسوا من رجال السلطة العامة، إضافة إلى ضمانات تتعلق بطبيعة عمل هذه المرحلة فهي قضائية صرفة وتقوم بها سلطة التحقيق عدا حالات استثنائية يتيح من خلالها القانون لسلطة جمع الاستدلال القيام بها ومنها حالة التلبس.

ومرحلة التحقيق في مجال الجرائم التقليدية تختلف عن مرحلة التحقيق في الجرائم المعلوماتية، لكون الإجراءات المطلوب اتخاذها في الثانية ذات طابع منطقي تقني تواجهها العديد من المشكلات التي قد تعيق القيام بها، بخلاف التحقيق في الأولى - الجرائم التقليدية - لطبيعتها المادية الملموسة وتنظيماتها التشريعية القائمة.

فما هي المشكلات التي تعيق إجراءات التحقيق في مجال الجرائم المعلوماتية سواءً ما يتعلق بالتفتيش، أم الضبط، أم الرقابة على الرسائل والمحادثات وغير ذلك من إجراءات التحقيق؟

ذلك ما سيتم الإجابة عليه في هذا المبحث.

المطلب الأول

التـفـتـيـش

يعرف التفتيش بأنه: (إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، يستهدف البحث عن الأدلة المادية لجريمة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه)[1].

ومن خلال هذا التعريف يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية، وبالتالي فلا توجد مشكلات تعيق إجراءه، لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة، حيث أن طبيعة الإجراءات المتخذة بشأنه مادية، تتمثل في الانتقال والدخول إلى المكان المراد تفتيشه[2].

بينما تفتيش نظم الحاسوب والشبكات يتم من خلاله البحث - في سر المتهم- عن أشياء مادية ومعنوية تفيد في كشف الحقيقة [3]. وبذلك فقد اجتمع العنصر المعنوي إلى جوار العنصر المادي، فهل يكون التفتيش في مثل هذا خاليا من المشكلات التي تعيق

---

(1) راجع سامي حسني الحسني، النظرية العامة للتفتيش في القانون المصري، دار النهضة العربية، القاهرة، 1982، ص244، وأحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، 1985، ص609، مشار إليهما في مؤلف محمد راجح نجاد، شرح قانون الإجراءات اليمني، مرجع سابق، ص221.

(2) يعد التفتيش من إجراءات التحقيق لكونه يتعلق بمرحلة أشد خطورة من مراحل جمع الاستدلال، حيث يتعرض للمساس بحقوق الأفراد وخصوصياتهم بالقدر الذي يقتضيه كشف أدلة الجريمة، ووفقا للضمانات والشروط القانونية التي تهدف إلى الموازنة بين حق الأفراد في خصوصياتهم، وحق المجتمع في كشف الجريمة وعقاب الجاني، ومع ذلك فقد وجد خلاف فقهي حول الطبيعة القانونية للتفتيش بين من يرى بأن التفتيش يعتبر من أعمال الاستدلال إذا تم القيام به في مرحلة جمع الاستدلال، وتم من خلاله الاقتصار على جمع المعلومات، ويعتبر من أعمال التحقيق إذا تم القيام به في مرحلة التحقيق وكان يهدف إلى البحث عن الأدلة وجمعها وكشف الحقيقة، وبين من يرى أن التفتيش يعد من إجراءات التحقيق في حالة أن تقوم به سلطة التحقيق سواء بصفة أصلية، أو عن طريق من ينيبها، ويكون من إجراءات الاستدلال حالة أن يخول القانون لمأمور الضبط القضائي القيام به دون مذكرة إذن بالتفتيش كما في حالة التلبس بالجريمة، وثالث يعتبر التفتيش من إجراءات التحقيق، بغض النظر عن السلطة التي تقوم به، ويعد الاتجاه الثالث هو الأصوب حيث يرى في التفتيش أجراء تحقيق فحسب تقوم به سلطة التحقيق بصفة أصلية ويقوم به مأموري الضبط في حالة التلبس أو الندب، لان التفتيش في الأساس هو إجراء تحقيق تقوم به في الأصل سلطة التحقيق وهي النيابة العامة في بعض الأنظمة أو المدعي العام في أنظمة أخرى، ومع أن القانون يجيز في حالات معينة القيام به من قبل مأمور الضبط القضائي- ضابط الشرطة القضائية- ومنها حالة التلبس بالجريمة فإن قيام المأمور به في مثل هذه الحالة إنما يكون بصفة استثنائية لا يغير من طبيعته القانونية في كونه إجراء تحقيق، وذلك يتفق مع نص المادة 138 إ.ج.ي.رقم 13 لسنة 1994.حيث تنص على أن (تفتيش المساكن عمل من أعمال التحقيق ولايجوز الالتجاء إليه إلا بمقتضى أمر من النيابة العامة بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جريمة معاقب عليها وفقا لقانون العقوبات النافذ.لمزيد من التفصيل حول طبيعة التفتيش راجع.هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص50، وص51. وراجع: شروقي محترف: التفتيش في قانون الإجراءات الجزائية الجزائري، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، 2005- 2008، ص6. كما أن المادة(44)إ.ج.ج رقم(06-22)المؤرخ في 20 ديسمبر2006 تتضمن عدم السماح لضباط الشرطة القضائية بإجراء التفتيش ما لم يكن لديهم إذن قضائي بذلك من وكيل الجمهورية، أو قاضي التحقيق.

(3)علي حسن محمد الطوالبة، مرجع سابق، ص12.

إجرائه؟ أم أنه توجد العديد من المشكلات التي ترافق تنفيذه في ضوء طبيعته غير المادية وكذلك الأدلة التي يهدف لكشفها والتي هي أيضا من طبيعة غير مادية؟

وبهذا الخصوص توجد العديد من المشكلات التي تعيق إجراء التفتيش، منها مشكلات تتعلق بمدى قابلية مكونات الحاسب الآلي والشبكات للتفتيش سواء المادية أم المعنوية، ومنها مشكلات تتعلق بالشروط الموضوعية والشكلية للتفتيش.

1- مدى قابلية مكونات الحاسوب والشبكة للتفتيش

يتكون الحاسب الآلي (Computer) من مكونات مادية (hard ware)وهي: الأشياء المادية الملموسة في جهاز الحاسوب وملحقاته، كما يتكون أيضا من مكونات غير مادية (Soft ware)[1]. وبخصوص تفتيش النوع الأول من المكونات- المادية- فلا توجد مشكلات تعيق القيام به، مثلها مثل أي مكونات مادية أخرى يتم تفتيشها بالطرق التقليدية وبموجب النصوص الإجرائية التقليدية، بخلاف تفتيش النوع الثاني – المكونات المعنوية للحاسوب- فهي التي يمكن أن تثير مشكلات، نظرا لطبيعتها المنطقية، وكذلك طبيعة إجراءات التفتيش التي هي من نفس الطبيعة المعنوية.

---

(1) يتكون الحاسب الآلي (computer) من مكونات مادية (Hard Ware)ومكونات منطقية (Soft ware) وتتكون المكونات المادية من:

- وحدات الإدخال (Input Unit) ووظيفتها استقبال البيانات المدخلة إلى الحاسوب وتمريرها إلى داخل الجهاز والتي منها لوحة المفاتيح (Keyboard) والفأرة (Mouse)ومشغل الأقراص (Disk Drive)والماسح (Scanner).
- وحدات الإخراج (Output Unit) والتي وظيفتها إخراج نتائج المعلجة وتشمل عدداً من الأجهزة منها، الشاشة (Screen) ، والطابعة (Printer) ومشغلات الأقراص (Disk Drives).
- وحدة الذاكرة (Memory Unit) وتقوم بتخزين البرامج والبيانات، وتنقسم إلى ذاكرة رئيسية أو عشوائية (Memory Random Access) (RAM) وتسمى ذاكرة القراءة والكتابة، حيث ومحتوياتها قابلة للتعديل والحذف والإضافة، وذاكرة قراءة فقط (Read Only Memory)(ROM) حيث يتم تخزينها بالبيانات المطلوبة أثناء التصنيع.
- وحدة الحساب والمنطق (Arithmetic and Logice Unit) وتقوم بإجراء العمليات الحسابية والمنطقية المطلوبة.
- وحدة التحكم (Control Unit) وتعمل على التحكم بوحدة التحكم وتنسيق تبادل البيانات والأوامر.
- وحدة الذاكرة المساعدة (Auxiliary Memory) .

أما مكونات الحاسوب المنطقية (Computer Software) فهي: مجموعة من البرامج والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات، وتنقسم إلى برامج تشغيل وهي ضرورية لتشغيل الجهاز وملحقاته ومندمجة في الجهاز ذاته، وبرامج تطبيق وهي تستخدم بحسب الحاجة والغرض الذي يريده المستخدم.

أما مكونات شبكات الحاسب الآلي فهي تتكون من اتصالات بعدية سلكية ولا سلكية على المستوى المحلي أو الدولي. وكل تلك المكونات تخضع للتفتيش المادي والمعنوي بحسب الأدلة المراد البحث عنها وكشفها وتجميعها.لمزيد من التفصيل حول مكونات الحاسب الآلي راجع: محند شريف بلعيد، هندسة ووظائف الكمبيوتر، الصفحات الزرقاء، الجزائر، 2001، ص27 وما بعدها، وراجع على محمد الطوالبة، مرجع سابق، من ص 17:ص24، وراجع عبد الله حسين علي محمود، جريمة السرقة في مجال المعلوماتية، مرجع سابق، ص369، وص370، وراجع أيضا: هلالي عبد ألاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، النسر الذهبي للطباعة، القاهرة،1999، ص17 وما بعدها.

كما توجد العديد من المشكلات التي لها علاقة بتفتيش أنظمة المعلوماتية وشبكات الحاسب الآلي فما هي تلك المشكلات ؟

أ- **مكونات الحاسب الآلي المادية**

يكاد الخلاف يتلاشى حول تفتيش المكونات المادية للحاسب الآلي (Computer) بحثا عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة، طالما تم القيام به وفقا للقانون، لأنه يقع على أشياء مادية منصوص عليها في القوانين الإجرائية ويتم عن طريقة ضبط الأدلة المادية المتعلقة بالجريمة، وبالتالي فإن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه الجهاز أو الأجهزة المراد تفتيشها، فيما إذا كان مكانا عاماً أو خاصاً ، فإذا كانت المكونات المادية للحاسوب موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه، حيث لا يجوز تفتيش تلك المكونات إلا في الحالات التي يجوز فيها تفتيش المسكن، أو المكان الخاص وبنفس الضمانات المقررة قانونا في التشريعات المختلفة، ونفس الأمر بالنسبة لوجود مكونات الحاسب في مكان عام فتطبق عليها قواعد وضمانات تفتيش تلك الأماكن والأشخاص إذا كانت في حيازتهم[1]، ومع أن تلك المكونات تخضع للنصوص الإجرائية التقليدية إلا أنه قد تم النص عليها ضمن نصوص حديثة لمواجهة الإجرام المعلوماتي[2].

---

(1) علي حسن محمد الطوالبة، مرجع سابق، ص28، عفيفي كامل عفيفي، مرجع سابق، ص343.

(2) ومن التطبيقات التشريعية التي تجيز تفتيش مكونات الحاسب الآلي من خلال ما تخوله بعض التقنيات الإجرائية لسلطة التحقيق من اتخاذ أي إجراء لازم لجمع الأدلة والحفاظ عليها المادة (251) من قانون الإجراءات الجنائية اليوناني، والمادة (487) من القانون الجنائي الكندي، كما توجد تشريعات قليلة تنص صراحة على تفتيش مكونات الحاسب الآلي ومنها التشريع الانجليزي الصادر في 29 يونيو 1990 والمطبق من 29اغسطس 1990 الذي يطلق عليه قانون إساءة استخدام الحاسب الآلي، فبالنسبة للجرائم المدرجة في القسم الثاني والقسم الثالث والتي تكون عقوبتها مدة لا تتجاوز خمس سنوات حبس - وهي جرائم الدخول غير المصرح به إلى النظام لتسهيل ارتكاب أفعال غير مشروعة، وجريمة التعديل غير المصرح به في نظام الحاسب الآلي- تجيز القبض على المتهم دون الحاجة إلى إذن قضائي Without warrant، كما تجيز تفتيش محل إقامة المتهم بحثا، عن أدلة مادية ذات قيمة تتعلق بالجرائم محل القبض، أما بالنسبة للجرائم التي لا تتجاوز عقوبتها ستة شهور، فإن التفتيش لا يكون إلا بإذن قضائي، بموجب دلائل قويه على اقتراف الجريمة، وأن ثمة أدلة يمكن الحصول عليها جراء التفتيش، كما أن القانون الكندي للمنافسة القسم الفرعي رقم 1/16 يزود الشخص الذي يحمل إذنا بالتفتيش إمكانية أن يستخدم أو يعمل على استخدام أي نظام للحاسب الآلي، لتفتيش أي بيانات يحتويها أو تكون متاحة، لهذا النظام كما يمكنه أن يسجل تلك البيانات في شكل مطبوعات أو مخرجات أخرى.راجع: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص73، وص74، وراجع أيضا: علي محمود حمود، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث منشور على شبكة المعلومات الدولية على موقع منتدى كلية الحقوق- جامعة المنصورة، ت.د 10/ 5/ 2007 على الرابط:
http://www.f-law.net/law/showthred.php?=1133

ولا يختلف القانونين اليمني والجزائري في هذه المسألة، من حيث جواز انطباق القواعد التقليدية في كلا القانونين على تفتيش مكونات الحاسوب المادية، حيث أن كلا القانونين قد تضمنت نصوص قانونية -سواءً تعلقت بالتحري أم التحقيق أم المحاكمة- تنطبق من حيث الأصل على تفتيش المكونات المادية للحاسوب، بهدف كشف الجريمة، وتجميع الأدلة[1]، مثل آثار الدماء وبصمات الأصابع والأقدام وغيرها من الآثار ذات الطبيعة المادية، إضافة إلى أن المكونات المادية للحاسوب وشبكة المعلومات والنظم لا تختلف عن غيرها من المكونات المادية الأخرى المسموح بتفتيشها للبحث عن الأدلة، وبالتالي لا يوجد ما يحول من تفتيشها.

كما أن أجهزة العدالة المخول لها القيام بإجراء التفتيش سواء بصفة أصلية، أو بصفة استثنائية يمكنها القيام بتفتيش المكونات المادية في الجريمة المعلوماتية دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية، مثلها مثل غيرها من المكونات المادية الأخرى.

وبناءً على ما سبق، فإن تفتيش الأدوات المادية لجهاز الكمبيوتر مثل لوحة المفاتيح أو الفأرة، أو الشاشة، وغيرها من الأشياء المادية الملموسة، وكذلك البصمات الموجودة عليها لا تدخل ضمن المشاكل الإجرائية التي تعيق إجراء التفتيش، إذ بالإمكان تطبيق النصوص التقليدية في القانونين اليمني والجزائري عليها، وبهذا فإن أجهزة الكمبيوتر التي يراد تفتيشها تخضع للقواعد التي تخضع له الأدوات المادية الأخرى، فإذا كانت في مسكن فإنه ينطبق عليها ما ينطبق على تفتيش المساكن، والتي منها مراعاة وقت التفتيش، والإذن بالتفتيش، والأشخاص القائمين على التفتيش، والأشخاص المطلوب حضورهم، ونوع من يتم تفتيشهم، ومراعاة الاختصاص المكاني، وعدم فض الأوراق المغلقة، وقد سبق إيضاح القواعد التي تتعلق بالتفتيش في حالة التلبس، ويتبقى القواعد المتعلقة بشروط وضمانات التفتيش سيتم إيضاحها لاحقا.

---

(1) ومن تلك النصوص التي اشتملت على القواعد الخاصة بالتفتيش ويمكن تطبيقها على تفتيش جرائم الحاسوب المادية المواد من(131- 144)إ.ج.ي، وكذلك المواد (45:47 ومن 79:85) إ.ج.ج.إضافة إلى المواد الخاصة بالتفتيش في حالة التلبس.

ب- مكونات الحاسب الآلي المعنوية

يشكل تفتيش مكونات الحاسب الآلي المعنوية إحدى أهم المشكلات التي تعيق إجراءات التحقيق، حيث أثارت هذه الصورة خلافا كبيراً في الفقه المقارن، لأن هذا النوع من التفتيش ينصب على بيانات وبرامج الحاسب الآلي التي تغيب فيها الطبيعة المادية، فليس لها أي مظهر مادي محسوس في العالم الخارجي.

ومع أن البعض يحاول التغلب على الصعوبة المتمثلة بكون البيانات المعالجة آليا ليس لها كيان مادي محسوس[1]، وبأن ذلك يمثل عائقا في إجراءات التفتيش للبحث عن الأدلة الإلكترونية، حيث يرون بأن تلك البيانات هي عبارة عن نبضات أو ذبذبات إلكترونية، أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة، ولها كيان مادي محسوس من خلال استشعارها وإمكانية قياسها، ولذلك يمكن إخضاعها لقواعد التفتيش التقليدية[2].

وبغض النظر عما إذا كانت وجهة هذا الرأي صائبة حسب تأكيد البعض بالاعتراف بالصفة المادية للبيانات المعالجة آليا[3]، فنحن لا نتفق معهم دون وجود نصوص قانونية تنظم ذلك، للمبررات التي سبق الإشارة إليها أثناء تناول جريمة السرقة في مجال المعلوماتية،إضافةً إلى ثمة معوقات إجرائية أخرى لتفتيش مكونات الحاسب الآلي غير المادية أهمها:

1) نقص الخبرة لدى السلطات التي تقوم بالتفتيش، حيث إن ذلك التفتيش يقتضي الولوج إلى الأنظمة المعلوماتية لضبط ما يعد صالحا من البيانات كدليل على ارتكاب الجريمة، وعملية الولوج للتفتيش وضبط البيانات تحتاج إلى إلمام بالجوانب التقنية.

---

(1) راجع عفيفي كامل عفيفي، مرجع سابق، ص344.

(2) وأبرز مثال على إمكانية تطبيق القواعد العامة للتفتيش على النظم المعلوماتية، قيام الفقه الكندي بالتوسع في تفسير نص المادة (487) كندي التي تقضي بإمكانية تفتيش وضبط أي شيء تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت، أو يشتبه في وقوعها، أو أنه سيتيح دليلا على ارتكاب الجريمة، أو أن هناك نية لاستخدامه في ارتكاب الجريمة، وكذلك فقد توسع قانون إساءة استخدام الحاسوب الانجليزي الصادر في 29يونيو1990، في النص على تفتيش نظم الحاسوب المادية والمعنوية، ونص أيضا على التفتيش في جرائم الولوج غير المصرح به على أنظمة الحاسوب، أو التعديل غير المصرح به في نظم الحاسوب بدون إذن طالما كان الهدف من الولوج ارتكاب أفعال غير مشروعة عن قصد، وبإذن قضائي في حالة أن يكون الولوج مجردا دون نية ارتكاب أفعال غير مشروعة.راجع:علي حسن محمد الطوالبة، مرجع سابق، ص33، عفيفي كامل عفيفي، مرجع سابق، ص346.

(3) عفيفي كامل عفيفي، مرجع سابق، ص344.

2) صعوبة تحديد محل التفتيش والأشياء المراد ضبطها، وذلك لتعلقها بأمور فنية تحتاج إلى أن يكون القائمون بالتفتيش على علم بذلك.

3) صعوبة السيطرة على الأجهزة المراد تفتيش أنظمتها، وخاصة عندما يكون الجهازان في مكانين مختلفين، ومتصلين بشبكة معلوماتية.

أما في حال وجود نصوص قانونية تنظم تفتيش مكونات الحاسب الآلي المعنوية فإن المشكلة التي تتعلق بمشروعية التفتيش تتلاشى، ويمكن الحد من باقي المشكلات عن طريق تدريب الجهات ذات العلاقة بالتحقيق في جرائم المعلوماتية، ومتابعة كل جيد في إطار التطور الرقمي في مجال التفتيش أو الضبط.

وإذا كان القانون اليمني لم يتناول تنظيم هذه المسألة ومازالت نصوصه التقليدية هي المعمول بها، لذلك ففي مثل هذه القضايا فإن الضحايا قد يلجأون أولا إلى الجهات الإدارية التي تقدم خدمات الإنترنت قبل متابعة الجهات القضائية بسبب قصور التشريع، كما أن الجهات الإدارية قد تقوم بالاستعانة بخبرات أجنبية لعدم توافر الخبرة في هذا المجال[1]، فإن القانون الجزائري قد تناول أحكام تفتيش نظم المعلوماتية، حيث أجاز لسلطة التحقيق القيام بإجراءات التفتيش في منظومة معلوماتية[2].

ج- مدى خضوع شبكات الحاسب الآلي للتفتيش

بالإضافة إلى كون تفتيش نظام الحاسب الآلي تعد ضمن الإشكاليات التي تعيق سير التحقيق، فإن تفتيش شبكات الحاسب الآلي تثير مشكلة قد تكون أشد خطورة من تفتيش نظام الحاسب الآلي حينما يكون مرتبطا بشبكة اتصال، وتثار مثل هذه المشكلة عندما يتعلق الأمر بنهاية طرفية (terminal) موجودة في منزل المتهم ومتصلة بجهاز يقع

([1]) ومن الأمثلة على ذلك ما حدث لموقع نيوز يمن – صحيفة يمنية – من تدمير لقواعد المعطيات وإتلاف كافة البيانات المخزنة في أرشيف الصحيفة الخاصة بها، حيث بادرت الصحيفة قبل اللجوء إلى القضاء بالشكوى لوزير المواصلات وتقنية المعومات والذي بدورة أبدى استعداد الوزارة للاستعانة بخبرات من الخارج بهدف الوصول إلى معرفة الجاني، ففي مثل هذه الحالة كان يمكن الاستغناء عن الخبرات الأجنبية في حال وجود خبرات وطنية من الجهات القائمة على الاستدلال والتحقيق وقبل ذلك وجو نصوص قانونية تعالج جوانب التفتيش والضبط في مجال المعلوماتية. لتفاصيل واقعة الاختراق والإجراءات التي تمت بشأنها راجع: موقع الصحيفة، 09/12/12على الرابط:

/http://www.newsyemen.net
http://www.newsyemen.net/view_news.asp?sub_no=1_2009_12_05_40003

(2) راجع: المادة (3) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الصادرة بتاريخ 2009/8/16،ع 47.

خارج منزل المتهم في نفس الدولة ومملوك لشخص غير المتهم [1]. كما تثار الإشكالية بصورة أكبر عندما يكون النظام المراد تفتيشه واقعا خارج الدولة، وتعد شبكة الإنترنت هي الشبكة الأهم التي تشكل عائقا في مجال التفتيش الجنائي من بين الشبكات المختلفة بسبب الانتشار الواسع لها، والعدد الهائل من البشر الذين يستخدمونها، والخدمات التي تقدمها في مجال الحياة المختلفة، والكم الهائل من البيانات والمواقع التي تتضمنها[2].

1) حالة جهاز متصل بجهاز المتهم داخل الدولة

تتمثل المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم، ويقع داخل الدولة، وتكمن المشكلة في تجاوز الاختصاص المكاني لسلطة التفتيش من ناحية، والاعتداء على خصوصيات الغير من ناحية أخرى.

وقد عالجت بعض التشريعات هذه المسألة [3] حيث نصت على إمكانية امتداد تفتيش المسكن إلى تفتيش نظام آلي موجود في مكان آخر، بغرض التوصل إلى بيانات تفيد في كشف الحقيقة، و بالتالي يجوز للقائم بالتفتيش أن يسجل البيانات الموجودة في النهاية

([1]) ومع أن امتداد التفتيش إلى جهاز غير الجهاز الذي يتبع المتهم، عندما يكون مرتبطا بشبكة اتصالات، أو في حالة أن يعمد المتهم تخزين البيانات في جهاز غير الجهاز الذي يتبعه، حتى لا يتم اكتشاف أمره- تعد من أهم المشكلات التي تعيق إجراءات التحقيق، فإن الفقه الألماني يرى أن بالإمكان امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني وذلك عندما يكون مكان التخزين الفعلي خارج المكان الذي يتم فيه التفتيش، كما تعرض مشروع قانون الإجراءات الهولندي لذلك صراحة، إذ نص في المادة 125 على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة في موقع آخر، شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة. راجع هلالي عبد اللاه أحمد، تفتيش نظم الحاسوب وضمانات المتهم المعلوماتي، مرجع سابق، ص77.وما بعدها.وعبد الله علي حسين محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، مقال منشور على شبكة الإنترنت، موقع منتدى كلية الحقوق، جامعة المنصورة، ت.د 2008/6/11 على الرابط

http//www.f-law.net/law/showthread.php?t=1312

([2]) تشير التقديرات البحثية في واقع الانترنت في العالم إلى أن 7.3 مليون صفحة تدخل الانترنت يوميا، وأن عدد الصفحات الظاهرة للعيان عبر مختلف مواقع الانترنت تقدر بحوالي 2.5 مليار صفحة وهي صفحات في متناول طالبيها في أي وقت، وأن الصفحات المخفية من حجم التعاملات المعروفة تقدر بزيادة عن الصفحات المعروضة العلنية ب 500 مرة أي ما يعني حوالي 1250 مليار صفحة متواجدة عبر الانترنت، ويقدر حجم البريد الالكتروني و النشرات الإخبارية المتداولة مجتمعة عام 2000 ب 1100 مليار رسالة، فيما شهد العالم عام 2005 وجود أكثر من 85 مليون موقع على الانترنت بزيادة تقدر ب 29% عن السنة التي قبلها أي عام 2004، وتقدر الصفحات الالكترونية المروجة لمواضيع إباحية ما مجموعه 372 مليون صفحة، برقم أعمال يقدر ب 57 مليار دولار مع أرباح سنوية تفوق ال1.5 مليار دولار، و تقدر الرسائل الجنسية المتبادلة عبر الانترنت ب 2.8 مليار رسالة جنس ودعارة أما توزيع الانترنت حسب اللغة فتشكل اللغة الانجليزية نسبة 78% من مجموع المادة المخزنة و 96 % من مجموع مواقع التجارة الإلكترونية، أما باقي النسب اللغوية فهي موزعة بين الإسبانية، الصينية، الفرنسية و العربية التي لا يتجاوز حجم استخدامها على صفحات الانترنت ال0.5 %. راجع: *تيطاوني الحاج*، الانترنت عملاق المعلوماتية، بحث مقدم إلى الملتقى الوطني الأول، القانون وقضايا الساعة- النظام القانوني للمجتمع الالكتروني، المركز الجامعي-خميس مليانة، ولاية عين الدفلى ، الجزائر، من9: 11 مارس 2008، ص7، ص8.

(3) المادة (25) من مشروع قانون جرائم الحاسب الهولندي. راجع محمد بن حاج الطاهر وعبد القادر دوحة، التحديات الأمنية والقضائية لمنع الجريمة الإلكترونية، مرجع سابق، ص169.

الطرفية التي يتصل بها النظام المعلوماتي، دون التقيد بالحصول على إذن مسبق من قاضي التحقيق، غير أن هذه السلطة مقيدة بقيدين اثنين هما :

الأول: ألا تكون النهاية الطرفية التي يرتبط بها الحاسب موجودة ضمن نطاق إقليم دولة أخرى.

الثاني: أن تحتوي النهاية الطرفية المرتبط بها الحاسب على بيانات تؤدي إلى كشف الحقيقة.

وإذا تم تلافي هذه المشكلة في الدول التي عدلت من تشريعاتها بحيث تخول لسلطة التحقيق إجراء التفتيش بالنسبة لهذا النوع من الجرائم في أي مكان داخل النطاق الإقليمي للدولة في حالة الضرورة وبعد أخذ الإذن بذلك، فلا زالت المشكلة قائمة في الدول التي لم تعالج المسألة من ناحية تشريعية، وذلك بخصوص التفتيش داخل النطاق الإقليمي للدولة بحيث يمكن معالجة هذه المشكلة من خلال تضمين التشريعات الداخلية نصوصا قانونية تتيح لسلطة المختصة إمكانية القيام بإجراء التفتيش لأي نظام يقع في النطاق الإقليمي للدولة وفقا لإجراءات معينة، كأن يتم إبلاغ الجهة القضائية صاحبة الاختصاص المكاني والموجود النظام المراد تفتيشه في نطاقها، وكذلك اخذ الإذن القضائي بممارسة الإجراء في اختصاص مكاني أخر.

وبالنسبة لموقف القانون اليمني من هذه المسألة فلا زال، يعمل بنصوصه التقليدية، والتي منها نص المادة(117)التي تم إيضاحها أثناء تناول الندب بحيث تتيح لعضو النيابة العامة إذا دعاه الحال لاتخاذ إجراء خارج نطاق اختصاصه تكليف عضو نيابة آخر للقيام بإجراء أو أكثر من إجراءات التحقيق[1]، وبالإمكان وفقا لما سبق التنويه تطبيق هذا النص على تفتيش أنظمة الحواسيب داخل الدولة، إلا أن ذلك سيكون مقصورا على تفتيش مكونات الحاسوب المادية.

أما القانون الجزائري فقد تضمن نصوصا قانونية إجرائية ضمن التعديل الأخير لقانون الإجراءات الجزائية[2] وسعت بعض الصلاحيات التي يمكن القيام بها من قبل سلطة التحقيق، ومن ذلك إمكانية قيام قاضي التحقيق بالتفتيش أو الحجز في أي وقت، وفي أي مكان على امتداد كامل التراب الوطني، أو يأمر ضابط الشرطة القضائية

(1) راجع المادة(117)إ.ج.ي رقم(13)لسنة1994.
(2) القانون رقم (06-22)المؤرخ في 20 ديسمبر2006.

المختص للقيام بذلك[1]، وبالتالي إمكانية القيام بإجراءات التحقيق في مجال الجرائم المعلوماتية في أي مكان داخل الإقليم الوطني للدولة.

ونظرا لوجود قصور في نصوص قانون الإجراءات الجزائية في تعديله الأخير 2006، حيث لم يتضمن التفتيش عن بعد، وتفتيش الكيانات المنطقية في نظام المعالجة الآلية للبيانات، فقد تم تلافي ذلك القصور بان سمح للسلطات القضائية المختصة، لمقتضيات التحريات والتحقيقات القضائية تمديد التفتيش عن المعطيات المبحوث عنها بسرعة إلى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني[2].

2) حالة جهاز متصل بجهاز المتهم خارج الدولة

وفي هذه الحالة فإن الإشكالية تثار بصورة اكبر في حالة أن يكون الجهاز المطلوب تفتيشه والمربوط بجهاز المتهم بنهاية طرفية يقع خارج الدولة، ففي الغالب يعمد مرتكبي جرائم المعلوماتية إلى تخزين البيانات الخاصة بهم- والتي تعد أدلة لإدانتهم في جرائم تم ارتكابها من قبلهم- خارج الدولة التي يقيمون بها، عن طريق شبكة الاتصالات البعيدة (Telecommunications network) بهدف عرقلة التحقيقات[3].

والتفتيش عن بعد أصبح مشكلة تواجه النظام الإجرائي ككل، حيث يتم إجراؤه من خلال الحاسوب ذاته، ولازال القانون الإجرائي اليمني خالياً من نصوص تتعرض لها بالتنظيم، إذ ليس من المستغرب أن يجد الشخص في حاسوبه ملفات غريبة ليس لها علاقة بالملفات الموجودة بنظامه أو البرامج التابعة له، وقد يكتشف- في حالة أن يكون لديه إلمام بالجوانب الفنية والتقنية للحاسوب- أن حاسوبه معرض للتفتيش في أي لحظة عن طريق تلك البرامج المزروعة على حاسوبه.

وتزداد خطورة الأمر حينما يتم استخدام برامج تمتلكها دول معينة متقدمة في مجال التكنولوجيا الرقمية، للتفتيش على أنظمة دول أخرى، لكونه لا يستند إلى مبرر

---

(1) انظر الفقرتين(الثالثة والرابعة) من المادة (47) إ.ج.ج رقم (06- 22) المؤرخ في 20ديسمبر 2006المُعَدِل والمُتَمِم لقانون الإجراءات الجزائية.(ج.ر 84، ص26،).

(2) راجع: الفقرة (ج) من المادة (4)، وكذلك الفقرتين الأولى والثانية من المادة(5) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(3) محمد عادل، خصوصية شبكة الإنترنت، مقال منشور على موقع كلية الحقوق- جامعة المنصورة، ت.د 2009/8/14، على الرابط:

http://www.f-law.net/law/showthread.php?t=1312

قانوني، ويشكل اعتداء على الخصوصية، فضلا عن كونه يجعل الدول عرضة للاعتداء في إطار جريمة التجسس عليها، إضافة إلى انتهاك حواسيب وخوادم في دول أخرى من قبل دولة ما[1].

وإذا كانت بعض التشريعات قد وسعت من صلاحيات سلطة التحقيق للقيام بتفتيش النظم خارج الإقليم وقرنت ذلك بحالة الضرورة، وإذا كان هذا الإجراء يفيد في كشف الحقيقة، إلا أن ذلك التوجه قد تم معارضته من قبل الفقه والقضاء في تلك الدول، باعتبار أن فيه مساسا بسيادة الدول ويجب التنسيق للقيام بذلك الإجراء[2].

وتفتيش مكونات وشبكات الحاسوب المعنوية وكذا النظم في القانون اليمني تشكل إحدى المشكلات التي تعيق إجراء التحقيق، ذلك أن نصوص التفتيش إنما تهدف إلى التنقيب عن الأدلة المادية التي تفيد في كشف الحقيقة، والتي تستند إلى عناصر مادية، إضافة إلى أن تطبيق تلك النصوص يقتصر على الأجهزة المتواجدة داخل الدولة لا خارجها.

ومع أن القانون الجزائري قد تلافى مشكلة التفتيش عن بعد خارج الإقليم الوطني أخير بموجب القانون رقم(09-04) لسنة 2009 من خلال مساعدة السلطات الأجنبية وفقا لمبدأ المعاملة بالمثل، وطبقا للاتفاقيات الدولية بهذا الشأن[3]، سنشير إلى ذلك بشيء من التفصيل أثناء تناول الاختصاص القضائي.

فهذه المشكلة تعد مشكلة دوليه لا يمكن الحد منها إلا في ظل تعاون دولي أو اتفاقيات دولية أو إقليمية، أو ثنائية، إضافة إلى تفعيل التعاون الدولي في مجال المساعدة

---

(1)عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص868، وص869.

(2) ومن التشريعات التي وسعت من صلاحيات سلطة التحقيق لإجراء التفتيش على نظم المعالجة الآلية للبيانات حتى لو كان النظام المراد تفتيشه يقع خارج الدولة القسم 103 من قانون الإجراءات الجنائية الألماني، والمادة (125) من مشروع قانون الإجراءات الهولندي، إلا أن بعض الفقهاء في هولندا تحفظوا بالقول بأنه قد يكون من الأفضل لأسباب علمية السماح بتفتيش نظام الحاسوب في بلد أجنبي بغرض ضبط البيانات المخزنة فيه، بيد أن هذا الاختراق المباشر وفقا لتقرير المجلس الأوربي يعتبر انتهاكا لسيادة دولة أخرى، ولذلك وفي ظل عدم وجود اتفاقية دولية يفضل عدم تطبيق نص تلك المادة، كما يعتبر بعض الفقهاء في ألمانيا أن تفتيش نظم الحاسوب المتواجدة في دول أخرى غير الدول التي يوجد المتهم بها يعتبر اختراقا لسيادة الدول، وخرقا للقوانين الوطنية والثنائية الخاصة في مجال العدالة القضائية، وقد أيد القضاء الألماني هذه الوجهة الفقهية، حيث لم تتمكن سلطات التحقيق في ألمانيا من الحصول على بيانات تم تخزينها في سويسرا عن طريق نهاية طرفية موجودة في المانيا متصلة بشبكة اتصالات في سويسرا إلا عن طريق المساعدة القضائية. راجع: هلالي عبد اللاه أحمد، تفتيش نظم الحاسوب وضمانات المتهم المعلوماتي، مرجع سابق، ص78، وعبدا لله علي حسين محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، مرجع سابق، على الرابط:
http//www.f-law.net/law/showthread.php?t=1312

(3) راجع: الفقرة الثالثة من المادة(5) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر 47 ص7.

القضائية، وتسليم المجرمين، في ظل خضوع جميع الدول لمبدأ المساواة، بحيث لا تقدم الدول المتقدمة في مجال التكنولوجيا الرقمية على السيطرة على أنظمة الغير والتجسس عليها وتفتيشها، ولا تطلق العنان لقوانينها لتخويل سلطات التحقيق فيها، من اتخاذ أي إجراء من إجراءات التحقيق حتى ولو تطلب ذلك الدخول على أنظمة الغير وتفتيش حواسيبهم.

2- شروط وضمانات التفتيش

نظرا لكون التفتيش يتضمن تقييداً للحرية الفردية ويمثل اعتداء على حرمة الحياة الخاصة، فيجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته ومنها: أن يتم صدور أمر قضائي مسبب بشأنه، وأن يباشر من قبل الشخص أو الجهة المختصة (النيابة العامة، أو مأمور الضبط القضائي في حالة ندبه، في غير حالات التلبس بالجريمة[1].

لذلك فقد تم إحاطة التفتيش باعتباره إجراء من إجراءات التحقيق بعدد من الضمانات التي تقيد القائمين به بعدم تجاوزها، حتى لا يساء استخدامه، وتنقسم تلك الضمانات إلى ضمانات موضوعية، وضمانات شكلية.

ومن الضمانات الموضوعية، ضمانات تتعلق بسبب التفتيش، وأخرى بسلطة التفتيش ذاتها، وثالثة تتعلق بمكان التفتيش والأشياء المراد تفتيشها وكذلك الأشخاص.

أما الضمانات الشكلية، فمنها ما يتعلق بمواعيد التفتيش، ومنها ما يتعلق بالأشخاص المطلوب حضورهم التفتيش، ومنها ما يتعلق بتحرير المحضر والضوابط الواجب مراعاتها أثناء ذلك. فهل تفي تلك الضمانات بتفتيش نظم الحاسوب والشبكات؟ أم أن تلك الضمانات لا تتناسب مع تفتيش النظم المعلوماتية؟

ولبيان ما تم ذكره يمكن القول بأن الضمانات التي فرضت لإجراءات تفتيش أشياء ذات طبيعة مادية قد تتحول إلى إشكاليات عندما يتم تطبيقها للتفتيش عن أشياء ذات طبيعة منطقية، ذلك ما سيتم إيضاحه في هذا الموضع .

---

(1) محمد أبو العلا عقيده، التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، من 26 نيسان (ابريل) 2003 : 28 نيسان 2003 ، ت.د 2009/1/30، موقع عرب قانون، وموقع مندى كلية الحقوق – جامعة المنصورة على الرابطين:
http://www.arblaws.com/board/archive/index.php/t-2275.html
http://www.f-law.net/law/showthread.php?t=2208
وراجع: سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المؤسسة الجامعية، الإسكندرية، 1979، ص488.

أ- الشروط الموضوعية

تتمثل الشروط الموضوعية التي يلزم تحققها لإجراء التفتيش، بسبب التفتيش المتمثل بوقوع جريمة، ونسبة ارتكابها إلى متهم، إضافة إلى ضرورة أن ينصب التفتيش على محل يحتمل العثور فيه على أدلة الجريمة، وأخير يفترض لكي يكون التفتيش صحيحا أن تكون له غاية تتمثل في أن يكون التفتيش بغرض العثور على الآثار والأشياء التي يمكن أن تفيد في كشف الجريمة[1].

1) أسباب التفتيش

تتمثل الضمانة الأولى من ضمانات إجراء التفتيش بقيام سبب يبرر ذلك الإجراء، وهو وقوع جريمة يتم بموجبها توجيه الاتهام إلى الشخص، أو الأشخاص المراد تفتيشهم بناء على دلائل كافية لاقتراف الجريمة ونسبتها إلى متهم أو متهمين محددين، عملا بقاعدة المشروعية "لا جريمة ولا عقوبة إلا بنص"، وبالتالي لا يجوز التفتيش من أجل فعل لا يشكل جريمة، وفي حالة عدم توافر الدلائل الكافية باقترافها ونسبتها إلى شخص أو أشخاص[2].

وسبب التفتيش بحثا عن أدلة الجريمة يعد ضمانة بالنسبة للجرائم التقليدية المنصوص عليها في القوانين، إذ بدون وجود السبب المتمثل في الجريمة، وبدون توجيه الاتهام لشخص أو أشخاص محددين فإن القيام بالتفتيش يعد إجراء باطلا[3].

وإذا كانت المشروعية متوافرة بالنسبة للجرائم التقليدية المنصوص عليها في القوانين، فقد لا تكون كذلك بالنسبة للجرائم المعلوماتية، في ظل الخلاف الفقهي حيال تطبيق النصوص التقليدية عليها، وفي ظل غياب التشريعات المستحدثة التي تجرم تلك الأفعال، ويترتب على ذلك انعدام السبب كمبرر للقيام بالتفتيش لعدم وجود جريمة، وفقا لمن ينادي بمواجهة تلك الجرائم بنصوص مستحدثة تتناسب مع كياناتها المعنوية كنتيجة منطقية.

([1]) راجع محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، مرجع سابق،ص223 وما بعدها، شروقي محترف، مرجع سابق، ص14 وما بعدها.

([2])علي حسن محمد الطوالبة، مرجع سابق، ص63، محمد راجح نجاد: حقوق المتهم في مرحلة جمع الاستدلال، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، دار المنار، القاهرة،1994، ص 451.

([3]) شروقي محترف، مرجع سابق، ص15.

أما من يقر بإمكانية تطبيق النصوص التقليدية على جرائم المعلوماتية فهو يقر إمكانية القيام بالتفتيش، بحيث يعتبر السبب في التفتيش أمرا محققا، وهنا تبرز المشكلة إزاء الخلاف في المسألة محل البحث، إذ لا يمكن تداركها في ظل الخلاف الموجود إلا بتعديل التشريعات وتضمينها الجرائم المعلوماتية بصورة صريحة.

ولا يكفي لقيام سبب التفتيش وقوع جريمة منصوص عليها في القانون، وتوجيه الاتهام لشخص أو أشخاص معينين فحسب، بل لابد من توافر أمارات قوية على وجود أشياء تفيد في كشف الجريمة[1]، وهذه الضمانة كسابقتها قد لا تجدي في مجال الجريمة المعلوماتية، بخلاف ما هي عليه في مجال الجريمة التقليدية، ذلك لأن التوصل إلى قرائن، أو أمارات قوية كسبب لقيام التفتيش غالبا ما تسبقها تحريات جدية، والتحريات في المجال المعلوماتي تلاقي صعوبات جمة وفقا لما تم الإشارة إليها ومنها نقص الخبرة لدى سلطة التحريات في مجال التحري في نظم المعلوماتية، مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها، و محوها، وتغييرها بكل سهولة وهذه بحد ذاتها تعد مشكلة تعيق إجراء التفتيش.

وتفتيش مكونات الحاسوب المادية في القانون اليمني والقانون الجزائري تتطلب توافر سبب للقيام به مثل أي مكونات مادية أخرى، ويتمثل السبب في وقوع جريمة وقيام قرائن كافية على وجود الدليل أو الأدلة محل البحث والتي تفيد في كشف الحقيقة، لدى شخص معين، أو في مسكنه، حيث نصت المادة(12)على ذلك بصوره صريحة بقولها " للمساكن ودور العبادة ودور العلم حرمة فلا يجوز مراقبتها أو تفتيشها إلا بمقتضى أمر مسبب من النيابة العامة وفق ما جاء بهذا القانون، ويجب أن يكون ذلك بناء على اتهام سابق موجه إلى شخص يقيم في المكان المراد تفتيشية بارتكاب جريمة معاقب عليها بالحبس على الأقل، أو باشتراكه في ارتكابها، أو إذا وجدت قرائن قوية تدل على أنه حائز لأشياء تتعلق بالجريمة، وفي جميع الأحوال يجب أن يكون أمر التفتيش مسببا". ونصت (135) من القانون اليمني كذلك على أن "للمحقق أن يفتش المتهم وله أن يفتش غيره إذا وجدت دلائل قوية أنه يخفي أشياء تفيد في كشف الحقيقة"، كما نصت المادة(138)على أن (تفتيش المساكن عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا

([1])هلالي عبد أللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص122.

بمقتضى أمر من النيابة العامة بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جريمة معاقب عليها وفقا لقانون العقوبات النافذ)[1].

و تطرق القانون الجزائري كذلك لسبب التفتيش في أكثر من نص، ومن تلك النصوص نص المادة(44) التي نصت على أنه (لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية، أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا بإذن صادر من وكيل الجمهورية أو قاضي التحقيق، مع وجوب الاستظهار بهذا الأمر قبل الدخول، إلى المنزل أو الشروع في التفتيش...)[2].

وفي هذه المسألة فإن المشكلة التي يمكن أن تثار بسبب تفتيش الحاسب الآلي وشبكة المعلوماتية بالنسبة لجرائم المعلوماتية تكون في الدول التي لم توجد فيها حتى الآن نصوص قانونية، أو قوانين تنظم مسألة تجريم تلك الجرائم وعقاب مقترفيها، لكون إجراء التفتيش لابد أن يبنى على سبب يتمثل بوقوع جريمة، وعلى سبيل المثال لم يتم تجريم جريمة الدخول أو البقاء في النظام المعلوماتي في القانون اليمني، وتبعا لذلك فإن اتخاذ إجراء من إجراءات التحقيق إزاء هذه الجريمة بما في ذلك التفتيش على نظم المعلوماتية قد يكون مصيره البطلان، طالما لم يتحقق السبب، ناهيك عما تتطلب الإجراءات التقنية في حالة النص على تلك الجرائم من نصوص تتناسب مع حداثتها.

ومع أن القانون الجزائري قد تضمن تجريم المساس بأنظمة المعالجة الآلية للبيانات[3]، إلا أنه مازالت العديد من الجرائم المتعلقة بالنظم المعلوماتية وشبكة الإنترنت خارجة عن نطاق التجريم مثل جرائم الاعتداء على المواقع الإلكترونية وحجبها، وتدميرها، وجرائم الاستغلال الجنسي للأطفال وغيرها من جرائم الإباحية، وكذلك تجريم التقاط البيانات أو اعتراضها، وبالتالي فإنه في نهاية الأمر ستخضع المسألة للنص التجريمي وتكييف القضاء للجريمة وقد تتخذ الإجراءات أو تهمل تبعا لذلك.

---

(1) المواد (12،و135،و138)أ.ج.ي رقم(13) لسنة 1994.

(2) المادة (44)إ.ج.ج رقم(22-06)المؤرخ في 20 ديسمبر 2006،(ج.ر84،ص6)

(3)راجع القسم السابع مكرر من قانون العقوبات الجزائري المعدل والمتمم بالقانون رقم(04 - 15)المؤرخ في 10نوفمبر 2004 والمتضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وقد تلافى المشرع الجزائري أخيرا ما يخص بعض الجوانب الإجرائية المتعلقة بجرائم المعلوماتية ومنها التفتيش، بحيث يمكن القول بتوفر سبب التفتيش، في الجرائم المعلوماتية المستحدثة والتقليدية وعدم الاقتصار على التفتيش في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المشار إليها في القسم السابع من قانون العقوبات الجزائري، وإنما يتعدى ذلك إلى كافة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث عرفها المشرع الجزائري بأنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[1].

لما تم ذكره فإن على المشرع اليمني تضمين قانون العقوبات نصوصا قانونية تعاقب مرتكبي الجرائم المعلوماتية التي تضمنتها تشريعات الدول المتقدمة وبعض تشريعات الدول العربية حتى يمكن القول بتحقق سبب التفتيش في حالة القيام به، وكذلك تضمين قانون الإجراءات الجزائية النصوص القانونية التي تتعلق بتفتيش أجهزة الحواسيب وأنظمة المعلوماتية، بحيث تتماثل مع النصوص التي وردت في القانون الجزائري والاتفاقيات الدولية، أو استحداث قانون موضوعي وإجرائي خاص في جرائم المعلوماتية.

2) المحل

يشترط كذلك لصحة التفتيش أن ينصب على محل، ويقصد بمحل التفتيش عند البعض[2]: بالمكان الذي يحتفظ فيه الشخص بأسراره المادية. وتبرير أصحاب هذا الرأي في أن التفتيش لا ينصب على الأسرار المعنوية، لأن الأسرار المعنوية يحتفظ بها الشخص في كمائن نفسه، وبالتالي فلا يمكن الحصول عليها بالتفتيش وإنما بطرق أخرى مثل الإستجواب، أو الاعتراف.

وإذا كان هذا الرأي يبدو صواباً قبل ظهور التكنولوجيات الحديثة، فإنه لا يبدو كذلك في ظل التكنولوجيا الرقمية وما رافقها من تخزين الكم الهائل من المعلومات بأنظمة المعالجة الآلية للبيانات، وما ترتب على ذلك من ظهور أدلة جنائية جديدة، ذات

---

(1) راجع الفقرة(أ) من المادة (2) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر 47 ص5.

(2) محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، مرجع سابق، ص224.

طابع معنوي وليس مادي، يمكن الحصول عليها بالتفتيش التقني لتلك الأنظمة، وكلما في الآمر تضمين ذلك في التشريعات القانونية.

ومحل التفتيش قد يكون منزلا، وقد يكون شخصاً وقد يكون محله رسائل، وقد تضمن القانون اليمني العديد من النصوص التي نظمت أحكام التفتيش، ومن ذلك نص المادة(135) حيث نصت على تفتيش الأشخاص بقولها (للمحقق أن يفتش المتهم وله أن يفتش غيره إذا وجدت دلائل قوية أنه يخفي أشياء تفيد في كشف الحقيقة).

ونصت المادة (136) على تفتيش الأماكن التي يحتمل أن يوجد فيها ما يفيد في كشف الحقيقة حيث نصت على أن (للنيابة العامة إذا توافرت القرائن الكافية أن تفتش أي مكان لضبط الأوراق والأسلحة، وكل ما يحتمل أنه استعمل في ارتكاب الجريمة التي يجري التفتيش بشأنها، أو نتج عنها، أو وقعت عليه، أو كل ما يفيد في كشف الحقيقة)

كما نصت المادة(138) إ.ج.ي على (تفتيش المساكن عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من النيابة العامة بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جريمة معاقب عليها وفقا لقانون العقوبات النافذ)[1].

وكذلك فقد نص القانون الجزائري على تلك الأحكام، حيث نصت المادة(79)على: (يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة، أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته)[2].

ونصت المادة(83)إ.ج.ج (إذا حصل التفتيش في مسكن المتهم فعلى قاضي التحقيق أن يلتزم بأحكام المواد من 45 إل 47 ..)[3].

([1]) المواد (135، و136، و138) من القانون اليمني رقم(13)لسنة 1994بشأن الإجراءات الجزائية.

([2]) المادة (79) من الأمر رقم (66-155) المؤرخ في 8يونيو 1966 يتضمن قانون الإجراءات الجزائية.

([3]) نصت المادة(83) من الأمر رقم (66-155) المؤرخ في 8يونيو 1966 يتضمن قانون الإجراءات الجزائية، على تفتيش المنازل حيث أحالت تطبيق إحكام تفتيش المنازل إلى المواد من 45 إلى 47 باعتبار أن تلك الأحكام قد تم تناولها في مجال التفتيش الذي يقوم به ضابط الشرطة القضائية، بموجب حالة التلبس، أو الندب للتحقيق، والضرورة وغيرها من الحالات المنصوص عليها في القانون، وتلك الأحكام يجب مراعاتها سواءً أكان القائم بالتفتيش مأمور الضبط أم قاضي التحقيق، والتي منها مراعاة القواعد الخاصة بحضور الأشخاص ملاك المنازل التي يجري تفتيشها سواءً كانوا متهمين أم يشتبه في وجود ما يفيد في كشف الحقيقة في منازلهم، أو من يمثلهم أو شهود، وكذلك القواعد الخاصة بمراعاة المدة الزمنية للتفتيش، وكيفية التعامل مع الأوراق والمستندات التي يتم ضبطها، والاستثناءات على تلك القواعد.

من خلال النصوص السابقة يتضح بأن القانونين اليمني والجزائري قد تضمنا أحكام تفتيش المنازل، بخلاف تفتيش الأشخاص حيث تضمنها القانون اليمني دون الجزائري، فلم يتضمن القانون الجزائري تفتيش الأشخاص سواءً أكان التفتيش وقائي، أم إجراء من إجراءات التحقيق باستثناء بعض مهام الضبط القضائي في إطار التحقيق الجمركي وفقا لنص المادة(42)من قانون الجمارك حيث أجاز لأعوان الجمارك، أن يقوموا بتفتيش الأشخاص في حالة الظن بأن الشخص يخفي بنية الغش بضائع ووسائل الدفع عند اجتياز الحدود، إلا أن ذلك لا يمنع من العمل بالقواعد العامة بهذا الشأن وهي قواعد تقوم على وجوب احترام حقوق الأفراد بعدم التعرض لها إلا في الحدود التي تقتضيها المصلحة العامة [1].

كما يجوز تفتيش الشخص كإجراء قضائي في حالتين:الأولى في حالة إلقاء القبض على المشتبه فيه، فجواز القبض على الشخص يجيز تفتيشه لأن إجراء القبض يعد اشد على حريات الأفراد من إجراء التفتيش[2].

والحالة الثانية: تفتيش الشخص كإجراء مكمل لتفتيش المسكن في حالة وجود دلائل تفيد في إخفاء احد المتواجدين في المنزل ما يفيد في كشف الحقيقة.

فهل تنطبق قواعد تفتيش المنازل والأشخاص على تفتيش نظم الحاسب الآلي؟

في هذه المسألة يجب التفرقة بين ما إذا كان التفتيش ينصب على الجوانب المادية للحاسوب، وبين ما إذا كان ينصب على الجوانب المعنوية.

ففي الحالة الأولى- في حالة أن ينصب التفتيش على الأشياء المادية- فإما أن يتم اعتبار الحاسوب جزء من المكان المرد تفتيشه وتضمين ذلك في إذن التفتيش فلا مشكلة على اعتبار أن الحاسوب جزء من ذلك المكان، وإما أن لا يتم تضمين تفتيش الحاسوب في آمر التفتيش، ففي هذه الحالة لا يدخل الحاسوب ضمن المكان المراد تفتيشه حسب رأى البعض[3] لأن الحاسوب متميز عن المحتويات العادية لمنزل المتهم ويتطلب الأمر تضمين الحاسوب، أو الحواسيب بدقة في إذن التفتيش.

([1]) راجع عبد الله أوهايبية، مرجع سابق، ص264، وص339.

([2]) راجع عبد الحميد ألشواربي، إذن التفتيش في ضوء القضاء والفقه، منشأة المعارف، الإسكندرية، بدون تاريخ طبعة، ص81. وراجع أحمد المهدي، التحقيق الجنائي الابتدائي وضمانات المتهم المعلوماتي، دار العدالة للنشر والتوزيع، القاهرة، بدون تاريخ طبعة، ص78.

([3]) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص855.

ومن جهتنا نرى بأن هذه المسألة تحتاج إلى تفصيل أكثر، ففي حالة أن تكون الأشياء المراد تفتيشها هي أشياء مادية ملموسة مثل قطعة السلاح التي ارتكبت بها الجريمة فلا يوجد ما يحول من التفتيش المادي للحاسوب بفتح الغطاء الخارجي لمعرفة ما إذا كان الجاني يخفيها فيه، وذلك بعد التفتيش في الأماكن الأخرى المحتمل وجود القطعة فيها، باعتبار التفتيش ورد على شيء مادي بحت يدخل في نطاق المكان والغاية من التفتيش، بخلاف ما لو تم تفتيش الحاسوب تفتيش معنوي من خلال الاطلاع على البيانات المدرجة فيه واتضح وجود معلومات تفيد باقتراف المتهم للجريمة ذاتها التي يتم التفتيش عن أدلتها،فإن التفتيش في هذه الحالة يكون باطلاً، لأنه انصب على محل غير المحل المراد تفتيشه.

فالتفتيش في مجال المعلوماتية والذي قد يشمل التفتيش على البرامج أو الكيانات المنطقية والبيانات المسجلة في ذاكرة الحاسب، أو في مخرجاته والسجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات، و دفتر يومية التشغيل، وسجل المعاملات، و السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة، يحتاج إلى نصوص قانونية مستحدثة تتناسب مع طبيعتها اللامادية[1].

وبهذا الصدد فقد عمل المشرع الجزائري على استحداث نصوص قانونية من خلالها يمكن السماح للسلطات المختصة بتفتيش الأنظمة المعلوماتية أو جزء منها، و المعطيات المخزنة بتلك النظم، وكذلك تفتيش أي منظومة تخزين معلوماتية، حيث جعلها محلا للتفتيش المعلوماتي ووسع من ذلك المحل بحيث لم يعد قاصرا على تفتيش أجهزة الحاسوب تبعا لتفتيش الأماكن والأشخاص، بل جعله يمتد ليشمل التفتيش عن بعد داخل النطاق الإقليمي للدولة إلى منظومة معلوماتية أخرى إذا كان هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة بالمنظومة الأخرى والتي يمكن الدخول إليها من المنظومة الأولى، كما جعل من صلاحيات سلطة التفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش، أو لدية علم بالتدابير المتخذة لحماية المعطيات

([1]) محمد أبو العلا عقيده، التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، مرجع سابق على الرابطين:
http://www.arblaws.com/board/archive/index.php/t-2275.html
http://www.f-law.net/law/showthread.php?t=2208

التـي تتضـمنها تلـك المنظومـة، لمسـاعدتها وتزويـدها بكـل المعلومـات الضـرورية لإنجـاز مهمة التفتيش [1].

أما في القانون اليمني فطالما لا توجد نصوص مستحدثة تعالج مشكلة محل التفتيش المعلوماتي فيتعين التعامل مع الحاسوب بموجب النصوص التقليدية بشرط أن يتم النص علـى تفتـيش بيانـات الحاسـوب وكياناتـه المعنويـة فـي أمـر التفتـيش، وأن يـتم ذلـك وفـق الضـوابط والقواعد الخاصـة بـالتفتيش والاسـتثناءات الـواردة عليـه مـع مراعـاة الجوانـب الفنيــة التــي تتميــز بهــا إجــراءات التفتــيش لتلــك الــنظم مــن ضــرورة وجــود الخبــراء المتخصصين في الجوانب الفنية والتقنية، ويمكن تطبيق ذلك على تفتيش الحواسيب تبعا لتفتيش المنـازل والأمكنـة، أو تبعـا لتفتـيش الأشـخاص، باعتبـار أن تفتـيش الشـخص يمتـد ليشمل الحقائب والأوراق، وأي شيء يحمله المتهم، فالتفتيش يشمل كل ما يتصل بجسم الإنسان باعتبار أنه من توابعه [2].

ويشترط في محل التفتيش، أن يكون معينا، وان يكون مما يجوز تفتيشه، فأما شرط أن يكون المحل معينا فنتيجة منطقية للمحافظة على حقوق وحريات الأفراد، إذ لا يمكن القيام بتفتيش حي بأكمله.

وأمـا شـرط أن يكـون المحـل ممـا يجـوز تفتيشـه فـلأن القـانون يسـتثني مـن التفتـيش أشـخاص ومحـلات معينـة مثـل منـازل وسـيارات وأشـخاص أعضـاء السـلك الدبلوماسـي، باعتبار أن هؤلاء الأشخاص وتلك الأمـاكن جـزء مـن أرضـهم ، وتطبيقـا لقواعـد القـانون الدولي ومبدأ المعاملة بالمثل [3]،

كـذلك يتمتـع أعضـاء المجـالس النيابيـة بالحصـانة مـن أن تتخـذ ضـدهم أو منـازلهم إجـراءات التفتـيش، بحيـث لا يجـوز أن يتخـذ نحـو عضـو مجلـس النـواب أي إجـراء مـن إجراءات التحقيق، أو التفتيش، أو القبض أو الحبس، أو أي إجراء جزائـي إلا بـإذن مـن

---

(1) راجع: المادة (5) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج.ر 47 ص6) .
(2) أحمد المهدي، مرجع سابق، ص.85.
(3) محمد راجح نجاد، مرجع سابق،ص227.

مجلس النواب عدا حالة التلبس وفي هذه الحالة يجب إخطار المجلس فورا، وعلى المجلس أن يتأكد من سلامة الإجراءات [1].

وكذلك توجد حصانة لمكاتب المحاميين من التفتيش، إذ أن هذه الأماكن يتم الاحتفاظ فيها بأسرار الدفاع والرسائل التي تتم بين المحاميين وعملائهم وقد تضمن القانون اليمني والقانون الجزائري بأنه لا يجوز للمحقق أن يضبط لدى ممثل الدفاع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمها المتهم إليهما لأداء المهمة التي عهد إليهما بها ولا المراسلات المتبادلة بينهما في القضية [2]. وبالتالي فإن مكاتب المحاميين والمراسلات بينهم وموكليهم لا تخضع للتفتيش حتى لو توافرت شروط التفتيش المشار إليها باستثناء أن يكون المحامي قد ارتكب جريمة، فإنه في هذه الحالة يخضع للتفتيش هو ومكتبة في حدود الغرض من التفتيش.

وما قيل عن الاستثناءات من قواعد التفتيش بالنسبة للدبلوماسيين وأعضاء المجالس النيابية، ومكاتب المحاميين، يمكن أن يقال عن أجهزة الحواسيب التابعة لهم سواء أكانت بصحبتهم(لابتوب)أو في منازلهم، أو على سياراتهم، كونها تعد جزاء من أمتعتهم تتمتع بالحصانة من التفتيش مثلها مثل سائر الأمتعة.

وإذا كانت تلك الأجهزة تتمتع بالحصانة من التفتيش الذي يفترض فيه قيام سلطة التفتيش بالانتقال المادي إلى المكان أو الشخص المراد تفتيشه، فكذلك الحال بالنسبة للتفتيش عن بعد، بحيث لا يمكن تبرير عدم القيام بهذا النوع من التفتيش بكونه يتم عن بعد ولا يتم بواسطته الاعتداء المادي على حرمة المسكن أو الشخص، حيث أن الاعتداء المعنوي على حرمة الحياة الخاصة أكبر بكثير من الاعتداء المادي على تلك الحياة، بسبب الكم الهائل من البيانات التي تحويها الحواسيب الشخصية، والتي يسهل الاعتداء عليها وكشفها.

3) الغاية من التفتيش

نظرا لخطورة إجراء التفتيش على الحياة الخاصة للأفراد باعتباره إجراء من إجراءات التحقيق، فلابد من أن يكون له غاية، إذ بدونها، وكذلك في حالة تجاوزها فإن

([1]) راجع: المادة(82) من دستور الجمهورية اليمنية المقر بتاريخ 2001/2/20.وكذلك المادة (110) والمادة (11) من الدستور الجزائري نوفمبر 1996 (ج.ر 76 ديسمبر1996، ص6 .

([2]) المادة (154)إ.ج.ي رقم (13) لسنة 1994، والمادة(45) إ.ج.ج رقم(06-22)المؤرخ في 20 ديسمبر 2006.

الإجراء سيكون باطلا، وبهذا الخصوص فقد تضمن ق.إ.ج.ي النص على ضرورة تحقق الغاية من التفتيش بقوله (لا يجوز التفتيش إلا للبحث عن الأشياء والآثار الخاصة بالجريمة التي يجري التحقيق بشأنها ولا يتجاوز إلى سواها إلا إذا ظهرت عرضا أثناء التفتيش أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة عن جريمة أخرى فيجوز لمن يقوم بالتفتيش ضبطها وإثباتها في المحضر)[1].

كما تضمن قانون إ.ج.ج النص على الغاية من التفتيش، حيث نصت المادة(81) على أن (يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة)[2].

وبناء على ذلك فلا يجوز التفتيش إلا للبحث عن الأشياء التي تعد حيازتها جريمة وتفيد في كشف الحقيقة ولا يتعداها إلى ما سواها، باستثناء أن يتم كشف جريمة أخرى على سبيل الصدفة، أثناء التفتيش، وعلى سبيل المثال في جرائم المعلوماتية، عندما يكون التفتيش من أجل ضبط برامج اختراق في جهاز الهاكر، فتظهر صور إباحية فإن الإجراء في هذه الحالة يكون صحيحا [3].

كما يجب حتى تتحقق الغاية من التفتيش في جرائم المعلوماتية، أن تتوفر أمارات وعلامات قوية، أو قرائن تدل على وجود أشياء أو أجهزة أو معدات معلوماتية في المكان أو لدى الشخص المراد تفتيشه، تفيد في إظهار الحقيقة[4].

وقد تضمن القانون الجزائري النص على الغرض من التفتيش في مجال المعلوماتية وأحال تفصيل ذلك إلى قواعد قانون الإجراءات الجزائية حيث نص على: (يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة(4) أعلاه[5]، الدخول، بغرض التفتيش ولو عن بعد، إلى:

---

(1)المادة (137)إ.ج.ي رقم(13)لسنة 1994.
(2) المادة(81) من الأمر رقم (66-155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية .
(3)راجع عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، ص856.
(4) هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص122.
(5) تضمنت المادة (4) من القانون رقم (09- 04) الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وهي نفس الحالات التي أشارت إليها المادة(5) بالحالات التي يجوز فيها تفتيش نظم المعلوماتية، وتشمل تلك الحالات على نوعين من التفتيش، منها تفتيش غرضه الوقاية من جرائم تكنولوجيا الإعلام والاتصال تدخل في إطار أعمال الضبط الإداري، وتفتيش غرضه مكافحة وكشف تلك الجرائم ومرتكبيها تدخل في مجال عمل الضبط القضائي، حيث تمثلت الحالات التي يجوز فيها التفتيش في مجال المعلوماتية بالحالات التالية:=

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية(1).

وبالتالي فإنه إذا ما تحققت الغاية من التفتيش وفقا لنصوص قانون الإجراءات الجنائية، فيحق للسلطات المختصة بالتحقيق الدخول إلى النظام المعلوماتي أو إلى جزء منه، بغرض التفتيش على ذلك النظام أو المعطيات المخزنة به، كما يجوز الدخول إلى نظام معلوماتي آخر داخل الإقليم الوطني أيضا بغرض التفتيش إذا ما تحققت الغاية منه، وذلك في حالة وجود أسباب تدعو للاعتقاد بأن المعطيات محل البحث عنها مخزنة في ذلك النظام.

ب- الشروط الشكلية

يعد إجراء التفتيش من الإجراءات التي فيها تعد على حقوق وحريات الإفراد، لذلك وكما سبق التنويه إلى أن ذلك قد قوبل في التشريعات المختلفة بوضع الضمانات والشروط التي توازن بين حق الفرد في المحافظة على حقوقه وحرياته من الانتهاك وحق المجتمع في الوصول إلى الجناة وعقابهم، عن طريق تخويل سلطات تحقيق العدالة القيام بالإجراءات الموصلة إلى ذلك ومنها التفتيش.

وتطبيق تلك الضمانات في مجال التفتيش على نظم المعلوماتية قد تتحول إلى مشكلات تعيق تحقيق الهدف من إجراءات التفتيش بدلا من كونها ضمانات في مجال التفتيش التقليدي.

وقد سبق الإشارة إلى الشروط الموضوعية لإجراء التفتيش ويتبقى الشروط الشكلية سيتم إيضاحها في هذا الموضع.

=

أ. للوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب. في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج. لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون أللجو إلى المراقبة الإلكترونية.

د. في إطار طلبات تنفيذ المساعدة القضائية الدولية المتبادلة

(1) الفقرة الأولى من المادة (5) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر 47 ص6.

1) تحديد أوقات التفتيش

من الضمانات الشكلية التي فرضتها النصوص التقليدية في اغلب قوانين الإجراءات الجزائية ضمانات تتعلق بمواعيد التفتيش بحيث يتم تحديد أوقات معينة للتفتيش، ويحظر القيام به خارج هذه الأوقات[1]، فيمنع التفتيش ليلا باستثناء حالات معينة نص عليها القانون.

وبهذا الخصوص فقد تم تحديد وقت تفتيش المنازل في القانون اليمني بالوقت المحدد من بعد شروق الشمس وقبل غروبها بموجب نص المادة(144)، ومع ذلك فقد أوردت المادة السابقة استثناءين على هذه الضمانة، الأول في حالة الجريمة المشهودة، والثاني في حالة مطاردة شخص هارب من وجه العدالة، بشرط أن يتم ذكر أسباب التفتيش ليلا في محضر التفتيش.

وفي حالة تعذر إجراء التفتيش ليلا لعدم توافر مبرراته يجوز اتخاذ الإجراءات المناسبة واللازمة لإحاطة المسكن ومنع أي شخص من مغادرته دون إذن حتى بدء التفتيش بعد شروق الشمس[2]

وحدد المشرع الجزائري الوقت المسموح به لتفتيش المنازل من قبل السلطة المختصة من الساعة الخامسة فجرا وحتى الثامنة مساء، حيث نصت الفقرة(1) من الماد(47) على أنه (لا يجوز البدء في تفتيش المساكن قبل الساعة الخامسة(5)صباحا، ولا بعد الساعة الثامنة(8) مساء، إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل، أو في ألأحوال الاستثنائية المقررة في القانون)[3].

([1])تنص المادة (144)إ.ج.ي على أن (تفتيش المساكن يجب أن يكون بعد شروق الشمس وقبل غروبها إلا في حالة الجريمة المشهودة أو مطاردة شخص هارب من العدالة)، وتنص المادة (47) إ.ج.ج رقم (6-22) المؤرخ في 20 ديسمبر 2006 (لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة(5) صباحا ولا بعد الساعة الثامنة (8)مساء إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الأحوال الاستثنائية المقررة قانوناً)راجع ج.ر 48،ص6.

([2]) راجع المادة (144) من القانون اليمني رقم (13)لسنة 1994 بشأن الإجراءات الجزائية.

([3]) الفقرة الأولى من المادة (47) إ.ج.ج رقم (06 -22) المؤرخ في 20 ديسمبر 2006،المعدل والمتمم لقانون الإجراءات الجزائية الجزائري (ج.ر48 ،ص6).

وكذلك القانون الفرنسي حيث حدد وقت التفتيش مابين الساعة السادسة(6) صباحا والساعة التاسعة مساء وفقا لنص الفقرة الأولى من المادة(59)إ.ج [1].

وبذلك فإن تلك النصوص قد هدفت إلى حماية حرمة حياة الأفراد ليلا، حيث يعد المسكن ملجأ حصينا لهم لا يجوز انتهاكه ليلا حفاظا على خصوصياتهم[2].

ومما سبق يتضح أن القانون اليمني لم يحدد وقت التفتيش بساعة محددة وإنما بوقتي الشروق والغروب، بينما حددت في التشريع الجزائري من الساعة الخامسة مساء حتى الثامنة مساء، وفي الفرنسي من السادسة صباحا حتى التاسعة مساء، وأرى دقة التوقيت في القانون اليمني لكونه ربطها بالظلام -الليل- وهو العلة أو القيد على إجراء التفتيش، لأن الوقت يختلف في الشتاء عن الصيف فقد تكون الثامنة مساء في الصيف نهارا، ويكون سكان المنزل مازالوا لم يخلدوا إلى الراحة والنوم، وقد تكون في الشتاء ظلاما وهو وقت يكون فيه قاطني المنزل قد خلدوا إلى مأواهم للراحة والنوم، ولا يمنع الأمر من تحديدها بالساعة شريطة أن يراعى في ذلك اختلاف التوقيت باختلاف الفصل.

ومع أن اشتراط تفتيش المنازل بوقت معين يعد ضمانة للمحافظة على خصوصيات الآخرين، فإن ذلك الشرط لم يؤخذ به على إطلاقه، حيث وردت العديد من الاستثناءات على تلك القاعدة تضمنت الخروج على الميقات الزمني في التفتيش بالنسبة لبعض الجرائم، وكذلك بعض الحالات مثل حالة الضرورة.

كما أن تطبيق ذلك القيد على نظم المعلومات والشبكات، قد يكون سببا في إخفاء الأدلة ومن ثم عرقلة سير التحقيق، لكون أدلة هذه الجرائم هي عبارة عن كيانات غير

---

(1)**Article 59**
(Ordonnance nº 60-1245 du 25 novembre 1960 art. 12 Journal Officiel du 27 novembre 1960)
(Loi nº 92-1336 du 16 décembre 1992 art. 12 Journal Officiel du 23 décembre 1992 en vigueur le 1er mars 1994)
(Loi nº 93-2 du 4 janvier 1993 art. 161 Journal Officiel du 5 janvier 1993 en vigueur le 1er mars 1993)
(Loi nº 93-1013 du 24 août 1993 art. 20 Journal Officiel du 25 août 1993 en vigueur le 2 septembre 1993)
"Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures".

(2) راجع: عبد الله أوهايبية، مرجع سابق، ص257، ومحمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، مرجع سابق، ص273.

مادية يمكن إخفاء أدلتها بسرعة غير متوقعة إذا ما علم الجاني مسبقا بالوقت الذي سيتم تفتيش أنظمته فيه، لذلك فقد تطرقت التشريعات الحديثة إلى إضافة جرائم المعلوماتية ضمن الجرائم التي تستثنى من قيد المدة الزمنية للتفتيش، وذلك ما ذهب إليه ق.إ.ج.ج في التعديل الأخير 2006.وسنتناول تلك الاستثناءات تباعا:

أ) طلب صاحب المسكن

يجوز لسلطة تفتيش المسكن - أصلية أكانت أم استثنائية - دخول المسكن لتفتيشه دون التقيد في الوقت المحدد إجراء التفتيش فيه، متى كان ذلك بطلب من صاحب المسكن، ولا يتطلب الأمر في هذه الحالة الحصول على إذن طالما كان التفتيش برضاء صاحب المنزل باعتبار أنه قد تنازل على القيد أو الضمانة التي نص عليها القانون برضاه واختياره، وقد تضمن هذا الاستثناء ق.إ.ج.ج [1]، ولم يتناوله ق.إ.ج.ي إلا أن مثل هذا الاستثناء لا يشترط أن يكون منصوصا عليه، طالما وقد تنازل صاحب الشأن عن ضمانة أو شرط وضعهما القانون لمصلحته.

ب) حالات الضرورة

كذلك فإنه يجوز في حالة الضرورة عدم التقيد بالمدة الزمنية لإجراء التفتيش، وقد نصت علي ذلك المادة(47) إ.ج.ج، وتتمثل في حالة توجيه نداء استغاثة من داخل المنزل، وهي حالات غير محددة على سبيل الحصر، إذ يمكن أن تقاس عليها كل حالة مشابهة لها [2].

كما تضمنتها نص المادة(149) إ.ج.ي بقولها (يجوز دخول أي مكان دون مراعاة الشروط الواردة في هذا الفصل وهذا القانون في حالة طلب المساعدة من الداخل، أو حدوث حريق أو غرق أو ما شابه ذلك من أحوال الضرورة).

ونرى بأن حالة الضرورة المشار إليها في النصين السابقين، لا علاقة لها بالتفتيش في الحالات الاستثنائية، لوضوح الغرض في مثل هذه الحالة، حيث يقتصر على الدخول لتلبية نداء استغاثة من الداخل، أو وجود ظرف يستدعي التدخل لمساعدة أصحاب الشأن كحدوث غرق أو حريق.

---

(1) راجع: الفقرة (1) من المادة (47) إ.ج.ج.
(2) عبد الله أوهايبية، مرجع سابق، ص259، وشيماء عبد الغني محمد عطا الله، مرجع سابق، ص401، ص402.

ج) جرائم التحريض على الأعمال الإباحية والاستغلال الجنسي للأطفال

كذلك تضمن ق.إ.ج.ج النص على جواز التفتيش قصد التحقيق في، جرائم التحريض على الفسق والدعارة التي يتم إرتكابها في الفنادق والشقق المفروشة والمحلات العامة التي يرتادها الجمهور، حيث نصت المادة(47) الفقرة (2) على (غير أنه يجوز إجراء التفتيش أو المعاينة أو الحجز في كل ساعة من ساعات النهار أو الليل بقصد التحقيق في الجرائم المعاقب عليها في المواد من 342 إلى 348 في ق.ع.ج وذلك في داخل كل فندق أو منزل مفروش، أو فندق عائلي، أو محل لبيع المشروبات، أو ناد، أو أماكن المشاهدة العامة وملحقاتها، وفي أي مكان مفتوح للعموم أو يرتاده الجمهور إذا تحقق أن أشخاصا يستقبلون فيه عادة لممارسة الدعارة)[1].

ولم يتضمن ق.إ.ج.ي النص على استثناء تلك الجرائم من القيد الزمني في إجراء التفتيش، إلا أنه يمكن القول بعدم وجود ما يمنع من القيام بتفتيش المحال العامة التي يرتادها الجمهور في أي وقت متى كان ذلك لازما للكشف عن الجريمة، وذلك لانتفاء العلة من التفتيش ليلا في مثل هذه الحالات طالما أنها مفتوحة في الليل أو النهار.

د) الجريمة المشهودة ومطاردة شخص هارب من وجه العدالة في القانوني اليمني

أضاف القانون اليمني حالتين وسع من خلالهما من الصلاحية المتعلقة بالمدة الزمنية للتفتيش، وتتمثل الأولى في حالة الجريمة المشهودة، والثانية في حالة متابعة متهم هارب، حيث نصت المادة(144)على (أ - تفتيش المساكن يجب أن يكون بعد شروق الشمس وقبل غروبها إلا في حالة الجريمة المشهودة أو مطاردة شخص هارب من وجه العدالة.

ب-يجب أن يذكر في محضر التفتيش أسباب التفتيش ليلاً .

---

(1) الفقرة(2) من المادة(47) من القانون رقم()06-22) المؤرخ في 20ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، حيث كان النص بموجب الأمر رقم(66-155) يجعل الاستثناء من القيد الزمني لإجراء التفتيش مقتصراً على جرائم التحريض على الفسق والدعارة المنصوص عليها في قانون العقوبات في المواد من 342- 348، وتم إضافة الجرائم المنصوص عليها في قوانين المخدرات إلى الجرائم التي يستثنى التحقيق فيها من القيد الزمني بموجب القانون رقم(82- 03)المؤرخ في 13 فبراير 1982 ، كما أضاف في تعديل أخر بموجب القانون رقم(95-10) المؤرخ في 25 فبراير 1995 جرائم الإرهاب والتخريب إلى تلك الجرائم التي تم استثناؤها من القيد الزمني في التفتيش، وفي التعديل الأخير 2006 أضاف المشرع الجزائري عدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.راجع فيما سبق(ج.ر 7،ص307،وج.ر11،ص 4،وج.ر48 ،ص6) وبالتالي فقد أصبح الاستثناء من ضمانة مراعاة عدم إجراء التفتيش ليلا يشمل عدد من الجرائم يمكن تصنيفها إلى جرائم التحريض على الإباحية والاستغلال الجنسي للأطفال، والجرائم ذات الخطورة والتي منها جرائم الإرهاب وتبييض الأموال، والجريمة المنظمة عبر الحدود الوطنية، وجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

ج: إذا امتنع إجراء التفتيش ليلا لعدم توافر مبرراته يجوز اتخاذ الإجراءات المناسبة واللازمة لإحاطة المسكن ومنع أي شخص من مغادرته دون أذن حتى بدء التفتيش بعد شروق الشمس)[1].

من خلال النص السابق يتضح بأن القانون اليمني قد أتاح لمأمور الضبط في حالة التلبس، أو لسلطة التحقيق القيام بإجراء التفتيش دون التقيد بالميعاد الزمني، ولم يتضمن ذلك القانون الجزائري بل على العكس من ذلك فقد أوجب القانون الجزائري في حالة تنفيذ أمر القبض عدم دخول مسكن أي مواطن قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءً.

وله أن يصطحب معه قوة لكي لا يتمكن المتهم من الإفلات من سلطة القانون [2].

و) تحديد الجرائم الخطرة

إضافة إلى ما سبق فقد تضمن ق.إ.ج.ج النص على استثناء عدد من الجرائم الخطرة على أمن المجتمع ولم يتضمنها القانون اليمني من ضمنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

فبعد أن حددت الفقرة الأولى من المادة(47) إ.ج.ج الوقت المسموح به لإجراء التفتيش، وبعد أن نصت الفقرة الثانية من ذات المادة على جوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات النهار أو الليل قصد التحقيق في جرائم التحريض على الفسق والدعارة واستغلال الأطفال جنسيا.

فقد تضمنت الفقرة الثالثة من ذات المادة النص على استثناء عدد من الجرائم الخطرة، حيث نصت على (عندما يتعلق الأمر بجرائم المخدرات، أو الجريمة المنظمة عبر الحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب، وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف الصحي فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني وغير سكني في كل

---

(1) المادة(144) من القانون رقم(13) لسنة 1994بشان الإجراءات الجزائية.

(2) انظر الفقرة (2) من المادة(122) من القانون رقم (06-22)المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية.

ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص)[1].

كما نص المشرع الجزائري على حالة خاصة يجوز فيه الخروج على القاعدة المتعلقة بالميعاد الزمني لإجراء التفتيش المنصوص عليها في المادة السابقة، حيث نصت المادة(82) على أنه (إذا حصل التفتيش في مسكن المتهم فعلى قاضي التحقيق أن يلتزم بأحكام المواد (من 45 إلى 47) غير أنه يجوز له وحده في مواد الجنايات أن يقوم بتفتيش مسكن المتهم في غير الساعات المحددة في المادة (47)، بشرط أن يباشر التفتيش بنفسه، وأن يكون ذلك بحضور وكيل الجمهورية)[2].

فالتفتيش وفقا لهذا النص لا يكون إلا من قاضي التحقيق أثناء التحقيق القضائي، وليس من ضابط الشرطة القضائية، ولا مجال هنا للحديث عن التلبس لكون الأمر يتعلق بالتحقيق بالجنايات حيث أن التحقيق فيها إجباري بموجب نص المادة(66)إ.ج.ج.

كما يشترط أن يكون التفتيش بحضور وكيل الجمهورية، وبالتالي فإنه قد تم توسيع صلاحيات قاضي التحقيق عن ضابط الشرطة القضائية، بالنسبة للجنايات إضافة إلى الجرائم السابقة التي تم الإشارة إليها ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب الإلكتروني وتبييض الأموال[3].

والمشرع الجزائري في تحديده للاستثناء الخاص بوقت التفتيش بجرائم المساس بأنظمة المعالجة الآلية للمعطيات يكون قد جعل ذلك الاستثناء قاصرا على تلك الجرائم المنصوص عليها في القسم السابع من قانون العقوبات دون غيرها من باقي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكان يجب على المشرع الجزائري طالما وقد وسع من صلاحيات سلطة الاستدلال والتحقيق حيال مكافحة هذه الجرائم من خلال القانون رقم (09-04) لسنة2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيا الإعلام والاتصال ومكافحتها، أن ينص على الاستثناء الخاص بعدم

(1)المادة (47) من القانون رقم (06-22)المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

(2) المادة (82) من الأمر رقم (66-155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

(3) شروقي محترف، مرجع سابق، ص27.

تحديد وقت التفتيش على تلك الجرائم أيضا لاشتراكهم في العلة وهي الخطورة وسرعة أخفاء أدلتها.

2) الأشخاص المطلوب حضورهم

كذلك توجد ضمانات تتعلق بالأشخاص المطلوب حضورهم التفتيش، كشرط حضور صاحب المكان المراد تفتيشه، حيث ذهب اغلب الفقهاء إلى ضرورة حضور المتهم التفتيش معتبرين ذلك من القواعد الأساسية التي يترتب على مخالفتها البطلان[1].

وقد نص على تلك الضمانات كلا من القانون اليمني والقانون الجزائري .

فنصت المادة(134) إ.ج.ي (يحصل التفتيش بحضور المتهم أو من ينيبه وبحضور شاهدين من أقاربه أو جيرانه، وإذا حصل التفتيش في منزل غير المتهم يدعى صاحبه للحضور بنفسه أو بواسطة من ينيبه وبحضور شاهدين من أقاربه أو جيرانه، ولا يجوز أن يكون الشاهدان من رجال التحقيق) [2].

كما نصت المادة(45) إ.ج.ج (إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.

وإذا جرى التفتيش في منزل شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش، وإن تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة...) [3].

كما تنص المادة(83) من ذات القانون على أنه: (إذا حصل التفتيش في مسكن غير مسكن المتهم استدعي صاحب المنزل الذي يجري تفتيشه ليكون حاضراً وقت التفتيش فإذا كان ذلك الشخص غائبا أو رفض الحضور أ ُجري التفتيش بحضور اثنين من

([1]) ومع أن جمهور الفقهاء في مصر قد اعتبروا حضور المتهم التفتيش من القواعد الأساسية، فإن محكمة النقض قد حذت اتجاها مخالفا لذلك وقضت بأن عدم حضور المتهم لا يترتب عليه البطلان مخالفة ما ذهبت إليه سابقا من القول بالبطلان.راجع: هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص164.

([2]) المادة (134) إ.ج.ي رقم (13) لسنة 1994.

(3)راجع: الفقرة (1، و 2) من المادة (45) من القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية.

أقاربه أو أصهاره الحاضرين بمكان التفتيش، فإن لم يوجد احد منهم فبحضور شاهدين لا تكون ثمة بينهم وبين سلطات القضاء أو الشرطة تبعية) [1].

ويلاحظ من خلال النصوص السابقة بأن القانونين اليمني والجزائري قد تطلبا لإجراء التفتيش حضور المشتبه به أو من يحوز أوراقا أو مستندات تفيد في كشف الحقيقة، أو من ينوب عنه أو يمثله، وقد تطلب القانون اليمني بجانب حضور المتهم حضور شاهدين من غير المعنيين بالتحقيق، بخلاف القانون الجزائري الذي لم يتطلب حضور الشهود إلا في حالة تعذر حضور المتهم أو من ينوبه، وبذلك فإن الضمانة المتعلقة بالحضور تكون أكثر فاعلية في القانون اليمني عنه في القانون الجزائري لتطلبها حضور شاهدين بجانب المتهم أثناء التفتيش.

كما يلاحظ بأن القانون الجزائري في نص المادة(83) إ.ج قد تطلب أن يكون الشاهدين - في حالة تعذر حضور صاحب المسكن- من أقاربه أو أصهاره الحاضرين بمكان التفتيش، ولا يلجأ للشاهدين من الغير إلا في حالة عدم وجودهما في عين المكان، وهي قاعدة لم يقرها في المادة (45) بالنسبة لضباط الشرطة القضائية حيث ترك لهم صلاحية اختيار الشاهدين متى كانا محلا لذلك [2].

وشرط طلب حضور شاهدين أثناء التفتيش المنصوص عليه في القانون الجزائري يتطابق مع ما هو منصوص عليه في القانون الفرنسي[3].

---

(1) الفقرة (1) من المادة (83) من الأمر رقم (66-155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم .

(2) راجع عبد الله أوهايبية، مرجع سابق، ص336.

(3) **Article 57**

(Ordonnance nº 58-1296 du 23 décembre 1958 art. 1 Journal Officiel du 24 décembre 1958 en vigueur le 2 mars 1959)

(Ordonnance nº 60-529 du 4 juin 1960 art. 1 Journal Officiel du 8 juin 1960)

Sous réserve de ce qui est dit à l'article précédent concernant le respect du secret professionnel et des droits de la défense, les opérations prescrites par ledit article sont faites en présence de la personne au domicile de laquelle la perquisition a lieu.

En cas d'impossibilité, l'officier de police judiciaire aura l'obligation de l'inviter à désigner un représentant de son choix; à défaut, l'officier de police judiciaire choisira deux témoins requis à cet effet par lui, en dehors des personnes relevant de son autorité administrative.

Le procès-verbal de ces opérations, dressé ainsi qu'il est dit à l'article 66, est signé par les personnes visées au présent article; au cas de refus, il en est fait mention au procès-verbal.

ومع ذلك فتوجد قوانين لا تتطلب حضور الشهود إلا في حالة أن يكون القائم بالإجراء ضابط شرطة قضائية، بخلاف ما لو كان القائم به قاضي التحقيق أو عضو النيابة العامة، فلا يلزم حضور شاهدين محل التفتيش في حال تعذر أو غياب صاحب المسكن(1).

وبالرغم من أهمية مثل هذه الضمانات التي تهدف إلى الاطمئنان على سلامة الإجراء وعدم التعسف في استخدامها(2) ، إلا أنها قد تتحول إلى مشكلات تحول دون الوصول إلى النتائج المتوقعة من إجراء التفتيش في حالة أن يكون التفتيش يخص إحدى جرائم المعلوماتية، بسبب أن إشعار المطلوب حضورهم التفتيش قد يتيح لهم التلاعب بالمعطيات والبرامج المراد تفتيشها، وبالتالي إخفاء أدلة الجرائم أو التلاعب بها، ومن ثم صعوبة التوصل إلى مرتكبيها، فقد يتم التلاعب بالأدلة وإخفائها عن بعد في الوقت مابين إجراءات إصدار الإذن بالتفتيش وموافقة المتهم بأن يتم التفتيش بحضوره.

لما تم ذكره فقد تنبه المشرع الجزائري لمثل هذا الأمر فلم يشترط في تفتيش عدد من الجرائم حضور المتهم أو صاحب المنزل المراد تفتيشه أو الشهود، ومن تلك الجرائم جرائم المخدرات، والجريمة المنظمة العابرة للحدود عبر الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالصرف الصحي (3).

وقد تم إضافة تلك الجرائم بموجب التعديل الأخير لقانون الإجراءات الجزائية 2006، حيث كانت النصوص السابقة تقتصر على استثناء جرائم الإرهاب والتخريب فقط، من قاعدة حضور المتهم أو صاحب المنزل أو من يمثلهما أو الشهود(4).

وما زال القصور في القانون الجزائري في عدم تضمين هذا الاستثناء على كل الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي منها جرائم المساس بأنظمة

---

(1) ومن تلك القوانين التي لا تتطلب حضور شاهدين لعملية التفتيش القانون المصري وذلك في حالة ما إذا كان القائم بالإجراء قاضي التحقيق أو عضو النيابة العامة، وكذلك مأمور الضبط قضائي في حالة الندب فقط حيث يحل محل النادب،.راجع: هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص164.

(2) محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، مرجع سابق، ص236.

(3) الفقرة الأخيرة من المادة (45) من القانون رقم (06- 22) المؤرخ في 20 ديسمبر 2006.(ج.ر 84 ،ص6).

(4) أضيفت الفقرة الأخيرة من المادة (54) من الأمر رقم (95- 10) المؤرخ في 25 نوفمبر1995 والتي بموجبها تم استثناء جرائم الإرهاب والتخريب من الخضوع للقواعد المتضمنة الأشخاص المطلوب حضورهم التفتيش. لمزيد من التفصيل حول شرح النص المشار إليه راجع أحسن بوسقيعة، التحقيق القضائي على ضوء قانون 26 يونيو 2001، ط2، الديوان الوطني للأشغال التربوية، الجزائر، 2002،ص92.

المعالجة الآلية للمعطيات التي أقتصر الاستثناء عليها فحسب، طالما وقد تم استحداث قانون في 2009 يتضمن القواعد الخاصة بالوقاية من جرائم الإعلام والاتصال ومكافحتها، وتضمن القواعد الخاصة بتفتيش نظم المعلومات والمعلومات المخزنة بها دون أن يشير إلى استثناء قاعدة الحضور في التفتيش.

أما قانون الإجراءات الجزائية اليمني فلا زال يفتقر لمثل هذه النصوص التي تنظم مسألة التعامل الإجرائي مع الجرائم المعلوماتية، فالنصوص المتعلقة بالأشخاص المطلوب حضورهم لم تتضمن استثناء جرائم معينة من الخضوع لضمانات الحضور، وأكثر من هذا فلا توجد نصوص قانونية سواءً موضوعية أم إجرائية تنظم التعامل مع تلك الجرائم .

ومع ذلك فقد ورد نص أخر يعطي الحق للمتهم في حضور جميع إجراءات التحقيق، واستثنى من ذلك حالة الضرورة والاستعجال، حيث نصت المادة (122) على أن (للمتهم أو المجني عليه أو ورثته أو من أصابه ضرر من الجريمة أو المطالب بالحقوق المدنية أو المسئول عنها ولوكلائهم – طبقا للقانون- أن يحضروا جميع إجراءات التحقيق وليس لهم الحق في الكلام إلا بإذن من المحقق وإذا كان المتهم مقبوضا عليه أو محبوسا وجب على المحقق إحضاره.

ومع ذلك فللمحقق أن يباشر في حالة الاستعجال بعض إجراءات التحقيق في غيبة الخصوم ولهؤلاء الحق في الإطلاع على الأوراق المثبتة لهذه الإجراءات، ويجوز للمحقق أن يجري التحقيق في غيبة الخصوم كلهم أو بعضهم إذا اقتضى الأمر ذلك، وليس لأي من الخصوم طلب إيقاف سير التحقيق بالطريقة التي قررها المحقق وعليه إطلاع من ذكروا على ما تم بمجرد انتهائه) [(1)].

وبالتالي فإن بالإمكان إعمال أحكام هذا النص فيما يخص عدم حضور المتهم التفتيش في الجرائم المعلوماتية، حيث يمكن للقائم بالتفتيش أن يستغني عن حضور المتهم، ومع ذلك فإن هذا النص لم يستثني الشهود من الحضور مما يجعل القائم بالتفتيش حتى في حالة الاستعجال أو الضرورة مقيدا بحضور الشهود.

---

(1) المادة (122) من القانون اليمني رقم (13) لسنة 1994 بشأن الإجراءات الجزائية.

3) محضر التفتيش

إضافة إلى الضمانات المتعلقة بموعد التفتيش وكذلك الأشخاص المطلوب حضورهم، فيشترط كذلك أن يحرر محضرا بالتفتيش يشمل الإجراءات التي تمت، وما أسفر عن التفتيش من أدلة، ويشترط فيه الكتابة، والتاريخ، والتوقيع، و اصطحاب كاتب يحرر المحضر ويوقع عليه مع المحقق.

حيث نصت المادة (150) إ.ج.ي بأنه (يجب على عضو النيابة القائم بالتفتيش أن يحرر محضرا بالإجراءات وما أسفرت عنه وما تم ضبطه من أشياء ويوقع عليه مع كاتب التحقيق [1].

كذلك فقد نصت الفقرة(2) من المادة(68) إ. ج. ج (وتحرر نسخة من هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل).

كما نصت الماد(79) من نفس القانون على (يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات) [2].

وتعود الحكمة من تحرير محضر التحقيق من قبل كاتب يتم اصطحابه لهذا الغرض، كي يتفرغ المحقق للعمل الفني المتمثل بالتحقيق نفسه لكي يستخلص منه الأدلة بحيث لا ينشغل بكتابة المحضر عن ذلك [3].

ولا يترتب على قيام المحقق بتدوين محضر التفتيش دون أن يستصحب معه كاتب لتدوين المحضر البطلان المطلق، لكونه لا يتعلق بالنظام العام، بخلاف إجراء التفتيش وتدوين المحضر بدون أذن قضائي بذلك، فذلك يتعلق بالنظام العام ويترتب عليه التمسك ببطلان الإجراء في أي حالة كانت عليها الدعوى[4].

ومحضر التفتيش في مجال الجرائم المعلوماتية إذ يشترط فيه أن يكون مكتوبا من قبل الكاتب الذي يجب اصطحابه مع المحقق، دون استلزام أن يكون لدية إلمام بالجانب

([1])المادة (151) إ.ج.ي.
([2]) الفقرة (2) من المادة (68) والمادة (79) إ. ج. ج.
(3) عبد الله أوهايبية، مرجع سابق، ص316.
([4]) راجع عبد الحميد ألشواربي، مرجع سابق، ص153.

التقني، يشكل مشكلة قد تعيق عملية التفتيش، حيث أن محضر التفتيش بالنسبة للجرائم التقليدية يختلف عن محضر التفتيش بالنسبة للجرائم المعلوماتية، فبالإضافة إلى ما يتطلبه المحضر بالنسبة للتقليدية من تدوين ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، على أن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره، وتوقيع محرره، والاستعانة بكاتب في كل الإجراءات التي تستلزم تحرير محضر، فإنه في الجرائم المعلوماتية فضلا عما ذكر لابد من إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات، ثم لابد أن يرافقه شخص متخصص في مجال الحاسب الآلي للاستعانة به في مجال الخبرة الفنية الضرورية، وكذلك المساعدة في صياغة مسودة المحضر بحيث تتم تغطية كل الجوانب الفنية في عملية التفتيش[1].

4) عدم فض الأوراق المختومة والاطلاع عليها

تضمن القانون اليمني والقانون الجزائري النص على عدم الإطلاع أثناء التفتيش على الأشياء التي تمس الأسرار الشخصية والعائلية، حيث نصت المادة (140) إ. ج. ي على: (أ- ليس للقائم بالتفتيش أن يضبط أو يطلع على الأشياء التي تمس الإسرار الشخصية أو العائلية للشخص حائز المكان الجاري تفتيشه أو الأشخاص الآخرين، وعلى من يقوم بالتفتيش أن يتخذ الاحتياطيات الضرورية لمنع انكشاف مثل هذه الأسرار.

ب: لا يجوز فض ما يوجد في مسكن المتهم أو غيره من أوراق مغلقة، ويباح عند الضرورة التحفظ عليها لعرضها على المحكمة المختصة لتفضها بنفسها) [2].

كما نصت المادة(84)إ.ج. ج على أنه (إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه ضرورات التحقيق وما توجبه الفقرة الثالثة من المادة (83).

ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في احراز مختومة .

(1) راجع هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص170.
(2) المادة (140) أ.ج.ي رقم (13) لسنة 1994.

ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه، أو بعد استدعائهما قانونا، كما يستدعى أيضا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء...)[1].

فمن خلال النصوص السابقة يتضح بأن القانونين اليمني والجزائري قد تضمنا حماية قانونيةً للأوراق المغلقة أثناء التفتيش، تتمثل بعدم فضها أو الإطلاع عليها إلا وفق ضوابط معينه بهدف الحفاظ على خصوصية الأفراد أثناء التفتيش للبحث عن الأدلة في الجرائم ذات الطابع المادي، ومن تلك الضوابط في القانون الجزائري أن الإطلاع على الأوراق المغلقة لا يكون إلا بالنسبة لقاضي التحقيق أو من يندبه لذلك من مأموري الضبط القضائي، وكذلك إحصاء الأشياء أو الوثائق ووضعها في احراز مختومة [2].

فهل يمكن اعتبار تشفير البيانات في الجرائم المعلوماتية بمثابة غلق للمستندات التي تم تشفيرها؟ وهل يكون بالإمكان تطبيق النصوص التقليدية الخاصة بالأوراق المغلقة على البيانات المشفرة الموجودة في النظام المعلوماتي؟

من المستقر عليه إجرائيا بأن النيابة أو جهة التحقيق تلتزم بعدم الإطلاع على الأوراق المختومة أو المغلقة الموجودة في المكان المراد تفتيشه وذلك لمظنة أن الغلق إنما يهدف إلى المحافظة على الأسرار الخاصة بالشخص المرد تفتيشه [3].

وإزاء القيد المتعلق بعدم جواز الإطلاع على الأوراق المختومة أثناء التفتيش فإن البعض يرى سريان القيد على ضبط محتوى أنظمة المعالجة الآلية للبيانات [4]، لأن العلة التي اقتضت تقرير هذا الحكم- عدم جواز الإطلاع على الأوراق المختومة أو المغلقة- بالنسبة للأوراق تتوفر بالنسبة لمحتوى نظام المعالجة الآلية للبيانات المحمي فنيا ضد الاطلاع غير المصرح .

فكما أن الغلق أو التغليف يضفي على تلك الأوراق مزيدا من السرية فكذلك التشفير يضفي سرية بالنسبة للبيانات المعالجة آليا وكذلك على برامج الحاسوب .

---

(1) أنظر المواد (83، 84) إ. ج. ج، وبالمقابل فقد تضمنت ذات المعنى المادة (52) إ.ج مصري، والمادة 58 إ.ج إماراتي.

(2) أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، 94.

(3) راجع موريس صادق، المشكلات العملية في الجرائم الجنائية، دار الكتب القانونية، بيروت، 2000، ص16.

(4)راجع، محمد فريد رستم، أصول التحقيق في جرائم الحاسوب، مرجع سابق، ص428، عبدا لله حسين علي محمود، السرقة في مجال المعلوماتية، مرجع سابق، ص347، ص348.

وحتى في حالة إقرار أن البرامج والبيانات المتعلقة بالخصوصية بمثابة الأوراق المختومة التي يجب عدم فضها والإطلاع عليها، ويدخل في مضمونها كل ما كان مشفرا أو محميا، فإن المشكلة في مثل هذه الحالة تكمن في أن المتهم أو الشخص المراد تفتيش أنظمته، أو نظامه المعلوماتي يكون بإمكانه إخفاء تلك المعلومات أو البرامج، أو التلاعب بها مما يتيح المجال أمامه لإخفاء أدلة الجريمة، وعلى وجه الخصوص إذا كان القائم بالتفتيش ليس لدية الإلمام الكافي لاتخاذ الإجراءات الفنية والتقنية المتطلبة لحفظ تلك البرامج والبيانات وتجميدها حتى يتم النظر بشأن مدى علاقتها بالجريمة محل التفتيش، ومن ثم القيام بالإجراءات التي تخول فضها والإطلاع عليها.

وبالتالي فإن معالجة مثل هذه المشكلة تكون من خلال أن يكون القائم بالتفتيش لدية التدريب الكافي في مجال التحقيق في جرائم المعلوماتية والبرامج الفنية المستخدمة في ذات المجال.

المطلب الثاني

إجـــــراءات ضبط مكونات الجريمة

تكون نتيجة التفتيش الصحيح المطابق لنصوص القانون ضبط كل ما هو ضروري لكشف الجريمة، وإيضاح كل ما يثير التباس بشأنها، وبخصوص المشكلات التي يثيرها ضبط مكونات الحاسب الآلي فيجب التفرقة بين ضبط المكونات المادية للحاسب الآلي والشبكات، وبين ضبط مكونات الحاسب الآلي المعنوية.

1- ضبط جهاز الحاسوب ومكوناته الرئيسية والفرعية

لا يثير ضبط مكونات الحاسب الآلي المادية أية مشكلات تعيق إجراءات التحقيق، وبالتالي لا يوجد خلاف بين فقهاء القانون في إمكانية ضبطها، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة وبالتالي فلا مشكلة طالما أن المكونات التي سيتم تفتيشها وضبطها هي في حقيقتها مكونات مادية، فلا توجد صعوبة في ضبط الدعامة المادية للبرنامج، أو الوسائل المادية المستخدمة في نسخه بطريقة غير مشروعة،

أو إتلافه بوسائل تقليدية كالكسر أو الحرق [1] ومن تلك المكونات التي يمكن أن تخضع للتفتيش والضبط:

- وحدة المدخلات (input unit): وتشمل لوحة المفاتيح (keyboard)، والفارة(mouse)، والقلم الضوئي (light Pen)، ونظام القراءة الضوئية للحروف (Optical character recognition system)، ونظام قراءة الحروف المغناطيسية (Magnetic ink character reader system).
- وحدة الحساب والمنطق (Arithmetic and logic unit): وتشمل مجموعة من الدوائر الإلكترونية والمسجلات.
- وحدة التحكم (control unit): وما تستعين به من مسجلات وسماعات منطقية.
- وحدة المخرجات (out unit): وما تشمله من وسائط كالشاشة، والطابعة، والرسم، والمصغرات الفيلمية.
- وحدة التخزين الثانوية (secondary storage unit) : بما تشمله من أقراص مغناطيسية (Magnetic disks) بأنواعها المرنة (Floppy disk)، والصلبة (Hard disk)، والأشرطة المغناطيسية (Magnetic tape).
- الأجهزة والوحدات الملحقة بالحاسوب لاستخدام شبكة الإنترنت كأجهزة المودم وأجهزة اختراق الاتصالات وتحليل الشفرات[2].

ولبحث مدى إمكانية تطبيق النصوص المتعلقة بالضبط في القانونين اليمني والجزائري على مكونات الحاسوب المادية، فلا نرى مانعا من تطبيقها، مثلها مثل غيرها من الماديات التي تفي النصوص التقليدية بمواجهتها موضوعيا و إجرائيا.

ومن تلك القواعد التي تتعلق بالضبط ويمكن تطبيقها على ضبط المكونات المادية للحاسوب : أن إجراءات الضبط هي من إجراءات التحقيق، بحيث لا يجوز ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق، ومن القاضي أثناء المحاكمة، وكذلك عدم جواز

---

(1)عفيفي كامل عفيفي، مرجع سابق، ص353، راجع أيضا: وليد عكوم، مرجع سابق منشور على شبكة المعلومات الدولية، على الرابط:

http://www.arablawinfo.com/Researches_AR/126.doc

(2) علي حسن محمد الطوالبة، مرجع سابق، ص140، هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص198.

ضبط الأشياء التي تمس الأسرار الشخصية أو العائلية للشخص حائز المكان الجاري تفتيشه، أو الأشخاص الآخرين، وإحصاء الأشياء المضبوطة التي تفيد في كشف الحقيقة، ووضعها في إحراز مختومة، وعند فتحها فإنه يستوجب حضور المتهم مصحوبا بمحاميه[1]، إضافة إلى كافة القواعد التي سبق ذكرها أثناء تناول التفتيش والتي منها: ضبط أي شيء يظهر عرضا ويكون مفيدا في كشف الحقيقة، أو يمثل جريمة أخرى، وكذلك عدم ضبط الأوراق والمستندات التي سلمها المتهم للمدافع عنه، أو الخبير الاستشاري لأداء المهمة التي عهد إليه بها، ولا المراسلات التي تمت فيما بينهما في القضية وغير ذلك من القواعد التي تم تناولها سابقا.

ومع أنه لا يوجد خلاف حول ضبط مكونات الحاسب الآلي المادية ومواجهتها إجرائيا بالنصوص التقليدية، مثلها مثل غيرها من الأشياء التي تساعد في إظهار الحقيقة، إلا أن بعض التشريعات قد ضمنت قوانينها النص صراحة على تفتيش تلك المكونات[2].

2- المكونات غير المادية للحاسوب

بالنسبة لمكونات الحاسب الآلي المعنوية فإن ضبطها يثير مشكلة وخلاف فيما بين الفقهاء بين من يرى بأن الضبط لا يرد إلا على شيء مادي أما الأشياء المعنوية - برامج وبيانات الحاسب المعالجة - فلا تصلح محلاً للضبط [3]، إلا إذا تم نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة، أو غير ذلك من الوسائل المادية، لأن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة فقط[4] ومن هذا الاتجاه الفقه الألماني واللوكسمبرجي[5].

ويرى أصحاب هذا الاتجاه بأن حل هذه المشكلة يكون عن طريق التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط، لتشمل البيانات الإلكترونية وبرامج الحاسب الآلي بجانب الأشياء المادية، وذلك بإضافة عبارة البيانات

([1]) راجع المواد (132، 140) إ. ج. ي رقم (13) لسنة 1994. والمواد من (44- 47 ، والمادة 84) إ. ج.ج لسنة 2006.

([2]) ومن القوانين التي نصت صراحة على تفتيش مكونات الحاسب المادية قانون إساءة استخدام الحاسوب الانجليزي الصادر في عام 1990، وقانون المنافسة الكندي، راجع: على حسن محمد الطوالبة، مرجع سابق، ص140.

([3])عبد الله حسين علي محمود، سرقة المعلومات المخزنة بالحاسب الآلي، مرجع سابق، ص 396 وما بعدها.

([4]) راجع: محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مرجع سابق، على الرابطين:
http://www.arblaws.com/board/archive/index.php/t-2275.html
http://www.f-law.net/law/showthread.php?t=2208

([5]) عفيفي كامل عفيفي، مرجع سابق، ص378، علي حسن محمد الطوالبة، مرجع سابق، ص145.

والبرامج المعالجة عن طريق الحاسوب إلى النص القانوني الذي ينص على التفتيش والضبط [1].

ومن يرى: إمكانية ضبط مكونات الحاسب الآلي المعنوية، لكون الغاية من التفتيش تتحقق بضبط الأدلة المادية التي تفيد في كشف الحقيقة، وهذا المفهوم يمتد ليشمل البيانات الإلكترونية، أو قاعدة البيانات [2]، ومن هذا الاتجاه الفقه الكندي، حيث يرى بأن الضبط إذا نظر إليه من خلال تطوره التاريخي، فإن الغرض منه في بادئ الأمر ضبط الأشياء المادية المحسوسة، أما الآن فالضبط لا يقتصر على هذا لغرض، وإنما يمتد إلى أغراض أخرى على رأسها الحصول على المعلومات والأدلة التي تتيح ضبط الأشياء، كما أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره، وذلك ما جعل بعض التشريعات تعدل من قوانينها وفقا لهذا الاتجاه ومن تلك القوانين القانون الكندي والقانون البلجيكي([3]).

ومع وجود خلاف حول خضوع المكونات غير المادية للحاسوب للضبط وفقا للنصوص التقليدية، فلا أحد يستطيع إنكار وجود المشكلات الإجرائية المتعلقة بضبط المكونات غير المادية للحاسوب، سواء تعلق الأمر بضبط برامج الحاسوب أو بياناته .

أ- برامج الحاسب الآلي(computer programs)

تكمن المشكلة في ضبط الأدلة التي يكون محلها استخدام وسائل فنية في نسخ أو إتلاف البرنامج كالفيروسات بسبب قلة خبرة مأموري الضبط القضائي وسلطة التحقيق في جمع الأدلة في هذا المجال، بخلاف ما لو تمت عملية النسخ أو الإتلاف بوسائل مادية، حيث لا توجد صعوبة في ضبطها.

كما تكمن المشكلة من ناحية أخرى حينما تتم عملية ضبط الوسائل التقنية المستخدمة في الإتلاف أو النسخ في الأنظمة والشبكات المعلوماتية الكبيرة، حيث ينتج

([1]) راجع :علي حسن محمد الطوالبة، مرجع سابق، ص146.
([2]) هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص199وما بعدها.
([3]) سار القانون الكندي وفقا للاتجاه الفقهي القائل بأن الضبط يشمل الأشياء المادية والمعنوية للحاسوب، حيث تضمن ضبط السجلات الإلكترونية من خلال الفقرة السابعة من المادة (29) من قانون الإثبات الكندي، كذلك فقد تضمنت المادة 39 من قانون تحقيق الجنايات البلجيكي، المدخلة في التقنين بمقتضى القانون الصادر في 23 نوفمبر سنة 2000، حيث يشمل الحجز وفقا لهذا النص على الأشياء المادية، وعلى البيانات المعالجة إلكترونيا راجع: عفيفي كامل عفيفي، مرجع سابق، ص378. وراجع أيضا: محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مرجع سابق. منشور على شبكة المعلومات الدولية.

عن عملية الضبط عزل النظام المعلوماتي بالكامل عن دائرته لمدة قد تطول أو تقصر وهو ما يسبب حتما أضرارا بالجهة مستخدمة النظام، ويترتب على ذلك عدم قيام مستخدمي الأنظمة المعلوماتية بالتعاون الكامل و الفعال مع سلطة التحقيق [1].

ب- بيانات الحاسب الآلي (computer data)

في هذه الحالة يوجد العديد من المشكلات تعيق ضبط البيانات (Data) التي تعد دليلا على ارتكاب الجريمة، منها عدم وجود دليل مرئي يمكن فهمه بالقراءة من طرف الضبطية القضائية، بالإضافة إلى عدم وجود آثار مادية يمكن على أساسها الاستدلال على وجود دليل على ارتكاب الجريمة، و يتجلى ذلك في جرائم الاختلاس والتزوير التي تستعمل فيها التقنية المعلوماتية، و حتى البيانات التي يمكن الوصول إليها يستطيع الجاني أن يدمرها في فترة زمنية قصيرة، ناهيك عن ضخامة البيانات التي يجب على المحقق فحصها مقارنةً بنقص الخبرة الفنية المتطلبة لعملية الفحص لتحديد البيانات التي تصلح كأدلة لإدانة للجاني من عدمه، و يزداد الأمر تعقيدا في حالة الأنظمة المعلوماتية المتصلة بنهايات طرفية أخرى تجاوز إقليم الدولة إلى إقليم دولة أخرى[2].

كما أن من المشكلات التي يمكن أن تثار بمناسبة ضبط البيانات المخزنة في جهاز الحاسوب مشكلة أخذ نسخة من تلك البيانات عند صعوبة ضبط النسخة الأصلية، وذلك في حالة أن تكون النسخة الأصلية مسجلة في النظام، أو بالشبكة التي تربط بين عدة أجهزة، حيث لا يمكن اعتبارها مثل النسخة الأصلية لاحتمال أن يكون قد تم التلاعب بها[3].

وكذلك فإن ضبط البيانات المعالجة آليا خارج النطاق المكاني لسلطة التحقيق، تعد من المشكلات الخطيرة التي تعيق إجراء التحقيق، ويترتب عليها إبطال الإجراء في حالة الدفع بعدم الاختصاص.

وهذه المشكلة بطبيعتها مرتبطة بمشكلة التفتيش خارج الاختصاص المكاني لسلطة التحقيق لكون الضبط في حقيقته ما هو إلا نتيجة من النتائج التي يهدف إليها التفتيش.

---

(1) راجع عفيفي كامل عفيفي، مرجع سابق، ص354.
(2) راجع .عفيفي كامل عفيفي ، مرجع سابق، ص 254، وص255.
(3) وتطبيقا لذلك فقد اعتبرت محكمة النقض الفرنسية بأن ضبط نسخة من البيانات المسجلة في الكمبيوتر وعدم ضبط الجهاز نفسه بما فيه من ذاكره تحتوي تلك المعلومات لا يعد من قبيل الضبط في مفهوم المادة 76 والمادة 97 من قانون الإجراءات الجنائية .راجع شيماء عبد الغني محمد عطا الله، مرجع سابق، ص429.

وإذا كانت بعض التشريعات ومنها التشريع الجزائري قد عالج بعض حالات امتداد إجراءات التفتيش والضبط خارج نطاق الاختصاص المكاني بالنسبة لبعض الجرائم، منها الجرائم الماسة بأنظمة المعالجة الآلية للبيانات، ويكون بذلك قد تغلب على المشكلة المتعلقة بالضبط أو التفتيش خارج نطاق الاختصاص المكاني لسلطة التحقيق(1)، إلا أن ذلك مقصور على نطاق الاختصاص داخل الإقليم الوطني، أما في حال أن يتطلب الأمر ضبط بيانات مخزنة بأجهزة أو نظم خارج الدولة فإن المشكلة ستظل موجودة، وكنتيجة منطقية بعدم قبول التفتيش لأماكن ومواطن ومواقع خارج صلاحية نظام العدالة المكانية(2)، فكذلك الضبط، وبالتالي فلا بد من وجود تعاون دولي في تنفيذ إجراءات الضبط والتفتيش في مثل هذه الحالة وذلك ما تداركه المشرع الجزائري أخيرا من خلال القانون رقم(09- 04) المؤرخ في 8 أغسطس 2009 للوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، إلا أن ذلك خاضع لمدى وجود اتفاقيات وتعاون دولي تجسد ذلك على الواقع.

كما أن من المشكلات التي يمكن أن تظهر في مجال ضبط البيانات تبرز عندما يكون المحقق بحاجة إلى معرفة معلومات معينة - في بعض القضايا - من شأنها تسهيل عملية الضبط أو التفتيش، كقاعدة البيانات (Data base) أو نظام إدارة قواعد البيانات (Data base management system) أو الفهرس (beadroll) أو التصميم التفصيلي للنظام (Detailed system design) أو فك الشفرة (code chap) في ظل قاعدة حق المتهم في الصمت، إذ من المسلم به كقاعدة عامة أن للمتهم أن يمتنع عن الإجابة على الأسئلة الموجهة إليه، حيث نصت على هذا الحق عدد من التشريعات(3).

---

(1) راجع المادة (16) والمادة (47) من القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري. وكذلك الفقرة الثانية من المادة (5) من القانون رقم(09 -04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها(ج.ر 47،ص6).

(2) عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، بدون رقم الطبعة ، ودار النشر، والتاريخ، ص498.

(3)ومن تلك القوانين، ق.إ.ج .ف قبل تعديله بالقانون(93-2) الصادر في 4 يناير 1993 حيث نصت الفقرة الأولى من المادة (114) منه على إلزام قاضي التحقيق بتنبيه المتهم عند حضوره أمامه للمرة الأولى، إلا أنه حر في عدم الإدلاء بأي إقرار، وعليه أن يشير إلى هذا التنبيه في محضر التحقيق، وكذلك ق.إ.ج الألماني حيث نصت الفقرتان الثالثة والرابعة من المادة(136) على التزام كل شخص يقوم باستجواب المتهم أن يبلغه بأن له الحرية في أن يدلي بأقواله بالنسبة للوقائع المنسوبة إليه، أو أن يحجم عن ذلك، كما أن التعديل الخامس في الدستور الأمريكي قد نص بعدم جواز إجبار أي شخص أن يشهد ضد نفسه .راجع: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص205.

وبتطبيق ذلك على الجريمة المعلوماتية فإن نتيجة تطبيق مبدأ عدم اتهام الشخص لذاته يضع حدود قوية على المدى الذي يكون فيه المتهم مجبرا في التعاون الفعال في التحقيقات المتعلقة بجريمته المعلوماتية[1].

كذلك فإن من المشكلات التي تتعلق بضبط بيانات الحاسب الآلي أن ضبط البيانات أو البرامج حتى في حال أن تم الضبط قد لا يتم الاحتفاظ بها وفق قواعد فنية يراعى من خلالها تحريز أقراص الحاسب الآلي التي تحوي البيانات وخاصة الأقراص المرنة[2]، مما يتسبب في محو أو إتلاف تلك البيانات.

وحيال ما تم ذكره فهل يمكن أن يتم تصنيف قانوني الإجراءات اليمني والجزائري ضمن الاتجاه القائل بإمكانية ضبط بيانات وبرامج الحاسوب وإمكانية تطبيق النصوص التقليدية عليها مثلها مثل الأشياء المادية؟ أم أن مقتضيات الواقع تتطلب تعديل نصوص قانون الإجراءات في كلا البلدين وتضمينهما كل ما يتعلق بضبط برامج وبيانات الحاسوب؟

وللإجابة على هذا التساؤل من خلال العودة إلى نصوص قانوني الإجراءات الجزائية اليمني والجزائري، نلاحظ بأنهما قد تناولا ضبط الأشياء المادية التي تفيد في كشف الحقيقة مقرونة بإجراء التفتيش باعتبار أن الضبط ما هو إلا أثر من آثار التفتيش.

وبهذا الخصوص فقد تم تناول أحكام الضبط ضمن الإحكام المتعلقة بالتفتيش[3] ومن تلك الأحكام:

([1]) في المجر لا يكون المدعى عليه مكرها بإثبات براءته، وفي مستهل استجوابه يجب أن يكون متنبها إلى أنه غير مجبر على الإدلاء بأي بيان، وبمقدوره أن يرفض الإجابة على الأسئلة أثناء الاستجواب، وبالتالي فإن المتهم لا يكون مجبرا على طبع سجلات الحاسب، أو الإمداد بالأكواد أو بكلمات السر، بل إن الشاهد يستطيع رفض الإدلاء بالمعلومات التي تدينه أو تدين أحد أقربائه، فيكون بإمكانه رفض طبع المعلومات التي يتم استرجاعها من ذاكرة الحاسب، كما أن مشروع قانون الإجراءات الجنائية في بولندا يقرر في المادة (63) على أنه لا يمكن إكراه المشتبه فيه أو المتهم على تقديم مطبوعات الحاسب، أو كشف الشفرات السرية، وفي اليابان فإن مالك الحاسب الذي تم استخدامه ليس عليه التزام التعاون الفعال، فلا يمكن إرغامه عن كشف كلمات السر أو مخرجات المعلومات. راجع: هلالي عبد اللاه أحمد، المرجع السابق، ص207.وراجع المادة (100) من الأمر رقم (66-155) المؤرخ في 8 يونيو 1966يتضمن قانون الإجراءات الجزائية.

([2]) من القواعد التي يفترض إتباعها للحفاظ على البيانات التي تم ضبطها وتحريزها في أقراص هي: عدم ثني القرص، وعدم تعريض القرص لدرجة حرارة مرتفعة أو منخفضة، بحيث تكون درجة الحرارة مابين 10درجات و52 درجة مئوية، وعدم ترك القرص يعرض للأتربة وذرات الغبار والدخان، ومنع تعريضها للمجالات المغناطيسية، إضافة إلى عدم لمس الأجزاء المكشوفة من القرص، وعدم الضغط على القرص بوضع أشياء ثقيلة عليه، وعدم تعريضها للأضواء أو لأي سائل من السوائل، ومنع كتابة البيانات على اللاصق بعد لصقها لأن الكتابة بالقلم قد تتلف القرص.

([3]) أنظر المواد (من131إلى 164) إ.ج.ي. والمواد من(44- 47) إ. ج.ج .

- عدم جواز ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق، ومن القاضي أثناء المحاكمة وفقا للقانون اليمني، ومن وكيل الجمهورية، أو قاضي التحقيق وفقا للقانون الجزائري.
- أن يقتصر الضبط على الأوراق والأسلحة و كل ما يحتمل أنه أستعمل في ارتكاب الجريمة، أو نتج عنها، أو وقعت عليه، أو كل ما يفيد في كشف الحقيقة.
- جواز ضبط الأشياء التي تظهر عرضا أثناء التفتيش و تعد حيازتها جريمة.
- وجوب إبراز الأمر الخاص بالضبط قبل الشروع فيه.
- عدم ضبط الأشياء التي تمس الأسرار الشخصية أو العائلية للشخص أو الأشخاص الجاري تفتيشهم .
- مراعاة القواعد الخاصة بالأشخاص المطلوب حضورهم، وبمواعيد التفتيش، وغيرها أثناء القيام بعملية الضبط، وكذلك الاستثناءات التي وردت عليها وتضمنها القانون الجزائري بصورة أكثر تفصيلا من القانون اليمني فيما يخص جرائم المساس بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب وتبييض الأموال، والمخدرات وغيرها من الجرائم التي تم الإشارة إليها أثناء تناول قواعد التفتيش.
- عدم جواز ضبط الأوراق والمستندات التي سلمهما المتهم للمثل الدفاع أو الخبير الاستشاري بغرض أداء المهمة التي عهد بها إليهما، وكذا المراسلات المتبادلة بينهما.
- تحرير محضر بالضبط، وبيان أوصاف الأشياء المضبوطة وحالتها وكيفية ضبطها، والمكان التي عثرت عليها فيه.
- غلق الأشياء المضبوطة والختم عليها، وإذا تعذرت الكتابة عليها فتوضع في كيس يوضع عليه شريط من الورق ويختم عليه.

ومن خلال أحكام الضبط المشار إليها أنفاً يتضح بأنها قد وضعت للتعامل مع الأشياء المادية المحسوسة وفقا لما تم التنويه له سابقاً، وأن كان القانون الجزائري قد أشار إلى عدد من الاستثناءات التي تتعلق بالضبط ومنها الاستثناءات المتعلقة بمواعيد التفتيش أو الضبط، والأشخاص المطلوب حضورهم في عدد من الجرائم منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مما قد يجعل القارئ يعتقد بأنه - أي القانون الجزائري- قد تضمن ضبط الأشياء المعنوية ذات الدلالة الرقمية التي تفيد في كشف

الحقيقة إزاء الجرائم المعلوماتية المرتكبة، ويزيد من تثبيت ذلك الاعتقاد بأن تعديل ق. إ. ج. ج قد تم في وقت قريب (ديسمبر 2006).

ومع ذلك فإن المتمعن في تلك النصوص يستنتج بأن قانون الإجراءات الجزائري لم يتضمن سوى ضبط الأشياء المادية التي تفيد في كشف جرائم المعلوماتية، بدليل أن الاتفاقية الدولية بشأن مكافحة الإجرام المعلوماتي، قد تضمنت مصطلحات جديدة تتناسب مع ضبط البيانات المعالجة، فمنحت السلطات القائمة بالتحقيق حق الضبط ولم تكتف بذلك المصطلح بل أوردت مصطلح أخر هو " أو الحصول بطريقة مشابهة على البيانات المعلوماتية"، وعدم تضمين المشرع الجزائري ذلك المصطلح يوحي بأن الضبط يقتصر على الأشياء المادية، باعتبار أن معظم التشريعات الحديثة قد عدلت نصوصها بما يتفق والخطوط العريضة التي جاءت بها الاتفاقية.

كما تضمنت الاتفاقية إجراءات جديدة تساعد على ضبط البيانات إن لزم الأمر ولم يتناولها القانون الجزائري، ومن تلك الإجراءات التحفظ العاجل على البيانات، أو المعلومات التي قد تفيد في كشف الحقيقة سوف نتناولها بشيء من التفصيل في المبحث الثاني من هذا الفصل.

وقد تنبه المشرع الجزائري لذلك القصور أخيرا من خلال إصدارة للقانون رقم(09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما وتضمينه القواعد الخاصة بضبط المعطيات المعلوماتية تحت مسمى حجز المعطيات المعلوماتية تضمنتها عدد من المواد[1] على النحو التالي:

- نصت المادة (6) على أنه :(عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة، تكون مفيدة في الكشف عن الجرائم ومرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

([1]) المواد (من 6- 9) من القانون (09 -04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ويجب في كل الأحوال على السلطة التي تقوم بالتفتيش أو الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات).

- المادة (7) (إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (6) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة).
- المادة (8) (يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك).
- المادة(9) (تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية).

كما أن المشرع الجزائري قد ألزم مقدمي الخدمات بجملة من الالتزامات في مجملها تساعد السلطات المكلفة بالتفتيش أو الضبط على ممارسة مهام التفتيش أو الضبط للكيانات المعنوية للحاسب الآلي عندما تستدعي ذلك ضرورة التحري أو التحقيق، وتخضع للقواعد العامة بقانون الإجراءات الجزائية، سيتم تناولها بشيء من التفصيل أثناء تناول دور الاتفاقيات الدولية في مواجهة المشكلات الإجرائية لجرائم المعلوماتية.

ومن خلال النصوص السابقة يتضح بأن المشرع الجزائري قد تلافى القصور في ضبط الكيانات المنطقية للحاسوب تحت مسمى حجز تلك الكيانات لتناسب كلمة الحجز مع الأشياء غير المادية.

وعلى المشرع اليمني أن يحذو حذو التشريعات الحديثة في مجال مكافحة الإجرام المعلوماتي، ومنها التشريع الجزائري ويضمن قانون الإجراءات الجزائية النصوص

القانونية التي تتيح لسلطة التحقيق الأصلية، أو الاستثنائية القيام بما من شأنه ضبط بيانات وبرامج الحاسوب، بهدف الوصول إلى كشف الجرائم المعلوماتية.

المطلب الثالث

ضبط الرسائل ومراقبة الاتصالات الإلكترونية

تعد الخطابات والرسائل والمحادثات الهاتفية من الأسرار الشخصية التي شملتها الحماية في أغلب التشريعات، ومن تلك التشريعات التشريع اليمني والجزائري، حيث كفلت النصوص الدستورية والقانونية في كلا البلدين تلك الحماية، وذلك بمنع الاطلاع عليها ، أو ضبطها سواء أكانت بريدية، أم برقية، أم هاتفية.

حيث نصت المادة(53) من الدستور اليمني على أن (حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي)[1].

ونصت المادة (39) من الدستور الجزائري على: (سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة)[2].

ونصت الفقرة (2) من المادة (12) إ .ج .ي على (حرية وسرية المراسلات البريدية والسلكية واللاسلكية وكافة وسائل الاتصال مكفولة وفقا للدستور، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر من النيابة العامة أو من المحكمة المختصة)[3].

ومن ناحية أخرى تجيز القوانين الإجرائية ضبط الرسائل ومراقبة المحادثات التلفونية وفقا لأحكام تحددها تلك القوانين في إطار حق المجتمع في الحفاظ على أمنه واستقراره، فهل تسري تلك الأحكام الإجرائية على المراسلات البريدية المستحدثة

(1) راجع: المادة (53) من دستور الجمهورية اليمنية المقر بتاريخ 2001/2/20.
(2) راجع:المادة (39) من الدستور الجزائري نوفمبر 1996 (ج.ر 76 ديسمبر1996، ص10.
(3) راجع : الفقرة (2) من المادة (12) من ق. إ ج. ي .

(electronic mail) والتصنت والمراقبة الإلكترونية لشبكات الحاسوب؟ أم أن تطبيق تلك الأحكام سيواجَه بالعديد من المشكلات المتعلقة بطبيعة الإجراء؟

1- البريد الالكتروني [1]

التعامل مع الرسائل الإلكترونية لا يختلف عن التعامل مع الرسائل الورقية، حيث يكون بمقدور الشخص أن يحتفظ بها أو يرد عليها، أو ينقلها إلى شخص آخر، ومع ذلك فتوجد مشكلات تثار بهذا الخصوص تتمثل في الخلاف حول طبيعة الرسائل الإلكترونية مقارنة بالرسائل الورقية.

فبينما يعتبرها البعض موجات كهرومغناطيسية لا تقارن بالمستند المادي مثل الرسالة المكتوبة، لأنها عبارة عن كيانات معنوية غير ملموسة[2]، ويترتب على ذلك اختلاف إجراءات ضبطها وتفتيشها حيث تحتاج إلى نصوص قانونية خاصة بها.

فإن البعض الآخر يعتبرها بمثابة المستند التقليدي، حيث إن التقدم التقني قد تجاوز المفهوم التقليدي للمستند الذي يعتبره مجرد ورقة مكتوبة ليس إلا.

فالمستند وفقا لأصحاب هذا الاتجاه هو: كل أسلوب لتحديد فكر أو فكرة على ورقة مكتوبة أو من خلال صوت أو صورة مسجلة، ولذلك يجب الاعتراف بها كمستندات[3].

ونتيجة لهذا الخلاف حول طبيعة الرسائل الإلكترونية فقد تضاربت بعض الأحكام حول تجريم الاطلاع عليها من قبل الغير من عدمه وفقا للنصوص التقليدية[4].

([1]) البريد الإلكتروني (electronic mail): هو وسيلة حديثة يتم من خلالها استخدام شبكة الحاسب الآلي في نقل الرسائل بدلا من الوسائل التقليدية، حيث يخصص لكل شخص بريد إلكتروني خاص به، وهذا الصندوق عبارة عن ملف على وحدة الأقراص الممغنطة يستخدم في استقبال الرسائل (Messages)، وقد ارتبط تطور البريد الإلكتروني(E mail) بتطور شبكة الاتصالات المعلوماتية، وتكمن أهميته في سرعته، وقلة تكاليفه، وسهولة نشره، فهو أكثر خدمات شبكات الإنترنت شيوعا واستخداما، إذ متى أصبح للمستخدم عنوان بريدي فإنه يستطيع استقبال وإرسال ما يريد من الرسائل في ثوان معدودة إلى أي جزء من العالم . راجع: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص213.

(2) راجع: علي حسن محمد الطوالبة، مرجع سابق، ص145.

([3]) ومن الاتجاهات التشريعية والفقهية التي تماثل بين المستند الإلكتروني والمستند الورقي قانون العقوبات الفنلندي بموجب تعديل1988 والذي بمقتضاه تمت المماثلة بين المستندات الإلكترونية والمستندات التقليدية، وفي البرازيل والمجر وشيلي ذهب الفقه إلى أن مفهوم المستند يمتد ليشمل أي شيء يختزن المعلومات من خلال التكنولوجيا وهو رأي في الفقه الفرنسي مشار إليه لدى هلالي عبد اللاه أحمد، المرجع السابق، ص214.

(4) حيث قضت محكمة دبي الابتدائية ببراءة متهم من تهمة فض الرسائل الإلكترونية الواردة إلى بعض موظفي مؤسسة الأمارات للاتصالات والمسجلة على البريد الإلكتروني للمؤسسة، عن طريق كسر الكلمات السرية التي تحول دون اطلاع الغير عليها، ونسخ صور منها على جهاز الحاسوب الخاص به، و بررت حكمها ببراءته في كون الرسائل المشار إليها في نص المادة(380) ع.ق لا تشمل الرسائل الإلكترونية على أساس أنها استخدمت بعد صدور القانون، إلا أن محكمة الاستئناف قد ألغت الحكم وأدانت المتهم بتهمة فض الرسائل الإلكترونية بدون رصا أصحابها بموجب النص التقليدي في قانون العقوبات ، حيث أن عبارة النص تتسع لكل الرسائل أيا كانت طريقة الإرسال، وقد أيدت الحكم محكمة التميز باعتبار أن نص قانون العقوبات يعاقب على فض الرسائل والبرقيات بغير رضا من أرسلت أليه، وهو ما يسري على البرقيات والرسائل سواء كانت مكتوبة أم مرئية أم مسموعة، مشار إليه لدى محمد عبيد الكعبي، مرجع سابق، 2004، ص226.

ولضبط الرسالة الإلكترونية (electronic mail) وفقا للإتجاه الأخير، فإن على المحقق اختيار صندوق البريد (Mail box) الخاص بالمتهم محل التفتيش من خلال القائمة الرئيسية لبرنامج البريد في الصفحة الشخصية والتي تظهر خلالها عدد من الخيارات منها صندوق الوارد (incoming box) وصندوق الصادر(Out box) وسلة المهملات.

وبالتالي فإن للمحقق أن يفتش أياً من مما ذكر بحسب الغرض من التفتيش، فإذا كان يريد ضبط الرسائل الإلكترونية التي وصلت للمتهم فعليه فتح صندوق الوارد في جهاز المتهم والاطلاع على الرسائل الواصلة إليه، وإذا ما أراد المحقق ضبط الرسائل الصادرة من المتهم فعليه فتح صندوق الصادر للاطلاع عليها، بينما في حالة ما إذا كان يريد ضبط رسالة قد ألغيت فعليه اختيار ملفات الحفظ أو سلة المهملات[1].

وقد طورت وسائل الاطلاع وضبط الرسائل الالكترونية في الدول المتقدمة تكنولوجيا، بحيث أضحت خاضعة للرقابة عن طريق برامج قد يشكل القيام بها اعتداء على الخصوصيات[2].

ولمعرفة وجهة نظر القانون اليمني والجزائري حيال المسألة محل الدراسة من خلال النصوص القانونية القائمة في كلا القانونين لمعرفة هل تم استحداث أو تعديل النصوص القانونية بما يتناسب مع ضبط الرسائل الإلكترونية، أم أن النصوص التقليدية تكفي لضبط تلك الرسائل؟

([1]) ومن القضايا التي تم ضبط الرسائل الإلكترونية فيها ومن خلالها تم التوصل إلى الجاني، قضية قتل في الأردن حيث قامت سلطات التحقيق المختصة بقراءة وطباعة المعلومات المخزنة على الهاردسك والأقراص المرنة، وكذلك طباعة الرسائل الإلكترونية (E- Mail) الخاصة بالمجني عليه من جهاز الحاسوب الذي كان يتبعه، والمحادثات التي تلقاها وتبين أنه تلقى تهديد عبر المحادثات الواردة إلى هاتفه، وكان ذلك سببا في التوصل إلى الجاني. كما وردت إحدى القضايا التي تم كشفها بواسطة البريد الالكتروني في الولايات المتحدة الأمريكية وبالتحديد في ولاية كاليفورنيا في عام 1999وتكمن في قيام أحد الأشخاص وصديقه بالتقاط صور فاضحة للأطفال والاتجار بها، حيث نتج عن التحقيق من خلال فحص المعلومات الرقمية المخزنة بالبريد الالكتروني الخاص بالمتهم وصديقه وجود شبكة دولية للاتجار بالصور الإباحية للأطفال، اتهم فيها ما يقارب من 200 متهم في 40 دولة.راجع :علي حسن محمد الطوالبة، مرجع سابق، ص151.

([2]) طورت إدارة التكنولوجيا التابعة لمكتب التحقيقات الفدرالية الأمريكية (F.B.I) برنامج كمبيوتر أطلق عليه اسم (كارنيفور) يقوم بتعقب وفحص رسائل البريد الإلكتروني المرسلة والواردة عبر أي حاسوب خادم تستخدمه أي شركة تقوم بتوفير خدمة الإنترنت، ويشتبه في أن تيار الرسائل المار عبر خدماتها يحمل معلومات عن جرائم وحوادث، حيث يتم تنفيذ عمليات التعقب والفحص بعد استئذان المحكمة المختصة بوضع أجهزة الشركة الموفرة للخدمة تحت الرقابة، كما يوجد برنامج أخر للرقابة على الصور المرفقة برسائل البريد الالكتروني هو برنامج(بورنزويير) ، وذلك بحثا عن أي شيء يثير الشبهة. راجع: مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة،2001، ص211، ص216.

بالرجوع إلى النصوص القانونية يلاحظ بأن القانون اليمني لازال يعتمد على النصوص التقليدية، بخلاف القانون الجزائري فقد ضمن في تعديله الأخير نصوصا تتناسب مع الجوانب التقنية لضبط الرسائل الإلكترونية.

ففي القانون اليمني لا توجد نصوص قانونية صريحة تعطي الحق لسلطة التحقيق في الاطلاع على الرسائل الإلكترونية وضبطها، وقد يتبادر إلى الذهن بأن النصوص التقليدية لا تفي بنفس الغرض، إلا انه ومن خلال الرجوع إلى تلك النصوص يتضح إمكانية تطبيقها على الإطلاع على الرسائل الإلكترونية وضبطها بصورتها المادية من خلال طباعتها أو تخزينها على وعاء مادي.

حيث نصت المادة (146)أ.ج.ي على أن (لعضو النيابة العامة المختص وحده الإطلاع على الخطابات والرسائل والبرقيات والأوراق الأخرى المضبوطة، على أن يتم ذلك بحضور المتهم أو الحائز لها أو المرسلة إليه وتدون ملاحظاتهم عليها، وله عند الضرورة أن يستعين في فحص الأوراق المضبوطة أو ترجمتها بكاتب التحقيق أو أحد مأموري الضبط القضائي أو المترجمين بحضوره وتحت إشرافه)

كما نصت المادة(148) من ذات القانون على أن (للنيابة العامة أن تأمر بضبط جميع الخطابات والرسائل والصحف والمطبوعات لدى مكاتب البرق....)[1].

فمن خلال هاذين النصين يلاحظ بأن المشرع اليمني قد خول لعضو النيابة العامة الإطلاع على الخطابات والرسائل المضبوطة، كما خول للنيابة العامة أن تأمر بضبط الخطابات والرسائل، فهاذين النصين وإن كانا قد وضعا لتخويل النيابة العامة حق الاطلاع وضبط الرسائل والخطابات المكتوبة، إلا أنه لا يوجد ما يمنع من تطبيقهما على الرسائل الإلكترونية بعد طباعتها أو حيازتها في وعاء مادي، للتشابه الكبير بين الرسالة الإلكترونية والرسالة الورقية، من حيث أن البريد الإلكتروني يحتوي على برامج متخصصة لكتابة وإرسال واستقبال واستعراض وتخزين الرسائل الإلكترونية، كما أن التعامل مع الرسائل الإلكترونية لا يختلف عن التعامل مع الرسائل الورقية حيث يكون بمقدور المستخدم أن يرد عليها أو يطرحها جانبا، آو يطبعها ويحفظها في ملف خاص[2]، أما إذا أراد عضو النيابة العامة أن يطلع على الرسالة من خلال التفتيش عن بعد

(1) راجع: المواد (146 و148) إ. ج. ي.
(2) علي حسن محمد الطوالبة ، مرجع سابق، ص 151

بموجب برامج اختراق أو تفتيش فأنه ينطبق في هذه الحالة ما ينطبق على التفتيش عن بعد وفقا لما تم ذكره أثناء تناول موقف القانون اليمني من التفتيش.

أما القانون الجزائري فقد أستحدث نصوصاً قانونيةً تتضمن مصطلحات تحمل مفاهيم تقنية تتناسب مع ضبط الرسائل الإلكترونية، بصدد عد من الجرائم في حالة التلبس، أو التحقيق الابتدائي منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وتتميز عن النصوص التقليدية في كونها تضمنت جوانب تقنية تسمح بمقتضاها لقاضي التحقيق أو ضابط الشرطة القضائية المناب أو المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور [1].

حيث نصت المادة(65 مكرر 5) على: (إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات، أو جرائم تبييض الأموال والإرهاب، أو الجرائم المتعلقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد، حيث يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية أو اللاسلكية، وتنفذ العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص، وفي حالة فتح تحقيق قضائي تتم العمليات المذكورة بناء على إذن من قاضي التحقيق[2].

كما نصت المادة المادة(3) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: (مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية)[3].

(1) تمم المشرع الجزائري الباب الثاني من الكتاب الأول بالقانون رقم (06 - 22) المؤرخ في 20 ديسمبر 2006، بفصل رابع بعنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور ويشمل المواد من 65 مكرر إلى 65 مكرر 10" (ج.ر 84، ص8).

(2) راجع: الفقرة الأولى من المادة (65 مكرر) من القانون رقم (06 - 22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية.

(3) المادة (3) من القانون رقم (09-04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومما تقدم يتضح بأن القانون الجزائري قد تميز عن القانون اليمني بتناوله إجراءات ضبط الرسائل من خلال نصوص مستحدثة، فهو وإن لم يشير بلفظ صريح إلى ضبط الرسائل الإلكترونية من خلال نص المادة (65-5 إ.ج) ونوه إلى أن إمكانية الضبط والاطلاع على الرسائل من خلال أعمال تقنية وفنية، بحيث يمكن وضع الترتيبات التقنية خارج المواعيد الرسمية للتفتيش أو الضبط وبغير علم ورضاء الأشخاص الذين لهم حق على تلك الأماكن، فقد تضمن بلفظ صريح ضبط الرسائل الإلكترونية من خلال نص المادة(3) من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أجاز لسلطة التحقيق بعد مراعاة القوانين التي تراعي سرية المراسلات ووفقا لقواعد قانون الإجراءات، الحق في الرقابة على الاتصالات وتجميع وتسجيل محتواها، مما يوحي بأن النص يشمل الرسائل الصوتية والمكتوبة.

كما أنه لم يقيد ذلك بمواعيد التفتيش والضبط، والأشخاص المطلوب حضورهم، بخلاف القانون اليمني الذي أشترط حضور صاحب الرسالة أو الحائز لها أو المرسلة إليه وإبداء ملاحظاتهم عليها.

2- التصنت والمراقبة الإلكترونية لشبكات الحاسب الآلي

تعد الرقابة على المحادثات الهاتفية من أخطر الوسائل التي يتم بواسطتها الاعتداء على الحق في الخصوصية، مثلها مثل تفتيش المنازل أو ضبط المراسلات والاطلاع عليها، لأن مراقبة المحادثات الهاتفية والاستماع إليها تتم دون علم صاحب الشأن، والتي من خلالها يتم سماع وتسجيل أدق أسرار حياته الخاصة.

و مازالت الرقابة على المحادثات الهاتفية محل خلاف في نظر الفقه في العديد من الدول[1]، حيث اختلف الفقه الجنائي في تكييف التصنت والمراقبة على المحادثات الهاتفية، فبينما يرى جانب من الفقه: أن ضبط المراسلات والتصنت على المحادثات الهاتفية يعتبر تفتيشاً لأنه ينطوي على المساس بحق السر، إذ أن من حق أي إنسان صيانة أرائه وأفكاره ورسائله بعدم اطلاع الغير عليها، وبالتالي فإن أي مساس بها يشكل مساسا بحق السر المصان بموجب القانون.

([1]) راجع: علي حسن الطوالبة ، مرجع سابق، ص155، وص156.وراجع أيضا: هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص217، وص218.

بينما يرى آخرون أن مراقبة المحادثات وتسجيلها هي من قبيل الملاحظة القضائية، إذ يشترط لممارستها وجود فائدة تتمثل في ظهور الحقيقة في جريمة تحقق فيها السلطة المختصة بالتحقيق ومع أنه إجراء يماثل طبيعة التفتيش إلا انه ليستفتيشاً .

ويرى جانب ثالث يتبناه الفقه الأمريكي بإمكانية اللجوء إلى تسجيل الأحاديث والتصنت وفق شروط منها: أن يتعلق الأمر بجريمة خطيرة مع وجود حاجة ماسة للجوء إلى هذا الأسلوب، وأن لا توجد بدائل أخرى تكون اقل مساسا بالحق في الحياة الخاصة، وأن يراعى الحذر الشديد عند اللجوء إلى هذا الأسلوب من خلال الفنيين وأصحاب الخبرة.

وإذا كان الأمر كذلك بالنسبة للتصنت والرقابة على المحادثات الهاتفية في صورتها التقليدية، فكيف يكون الأمر بالنسبة للرقابة والتصنت على شبكات الحاسب الآلي في ظل التقنية الرقمية التي تحتاج إلى جوانب فنية تقنية في مجال الرقابة، ومدى شرعية تلك الإجراءات في ظل النصوص القانونية الإجرائية التقليدية؟.

ولإيضاح ذلك فنرى أنه لا يوجد ما يمنع من تطبيق النصوص التقليدية في مجال المراقبة والتصنت الالكتروني على شبكات الحاسوب بالنسبة للمحادثات التي تتم عبر شبكات الحاسوب، طالما أن النتيجة واحدة وهي سماع تلك المحادثات والاحتفاظ بها كدليل على ارتكاب الجريمة، بالإضافة إلى أن شبكات الحاسب الآلي تستخدم ضمن استخداماتها خطوط الهاتف، فالاختلاف لا يكون إلا في الوسيلة المستخدمة، وبالتالي فإذا ما تم مراعاة النصوص القانونية وفقا للضوابط الواردة فيها من اقتصار ذلك الإجراء على سلطات معينة، غالبا ما تكون هي سلطة التحقيق، وبشروط معينة تراعى من خلالها الحفاظ على الحق في الخصوصية بالقدر اللازم الذي لا يتعارض مع تحقيق العدالة.

وتظل المشكلة في هذا الشأن متعلقة بالرقابة على المعطيات الموجودة أو التي يتم تبادلها بواسطة الشبكة بموجب النصوص التقليدية، وكذلك عدم توافر الخبرات الفنية والتقنية اللازمة في الدول التي مازالت متأخرة في المجال التكنولوجي.

وما تم ذكره يقتصر على الرقابة القضائية، أما الرقابة التي يقوم بها رب العمل على المحادثات أو المعطيات الموجودة في شبكة الحاسوب التابعة له، فقد اعتبر البعض أن ذلك يعد من قبل الرقابة المشروعة وقد قضت بذلك بعض المحاكم الأمريكية[1].

بينما خالف ذلك القضاء الفرنسي، حيث لم يسمح لرب العمل بمراقبة المحادثات التلفونية للعاملين[2].

أما عن موقف نصوص القانون اليمني والجزائري حول التصنت والمراقبة الإلكترونية لشبكات الحاسوب والإنترنت.

فهي تتمثل بالنسبة للقانون اليمني بعدم تضمينه ألفاظا صريحة تشير إلى التصنت الإلكتروني والرقابة على شبكات الحاسوب والإنترنت، وإنما تضمنت الرقابة على المحادثات الهاتفية من خلال عدد من الأحكام[3]. منها:

- جواز تكليف أحد رجال إدارة الهاتف بعد تحليفه اليمين القانونية بالاستماع إلى المحادثات الهاتفية وتسجيلها، وذلك بموجب أمر من رئيس النيابة المختص لنقل مضمونها إليه.
- أن يتضمن الأمر تحديدا واضحا ودقيقا للمكالمة المطلوب تسجيلها في خلال مدة 30 يوما من تاريخ صدور الأمر.
- جواز مراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيل لأحاديث تجرى في مكان خاص متى كان ذلك لازما لكشف الجريمة.
- في جميع الأحوال يجب يكون الأمر مسببا ولمدة لا تزيد على ثلاثين يوما.
- أن تتوافر باقي أحكام التفتيش المشار إليها من تحرير المحضر، والمحافظة على عدم كشف الأسرار التي تتعلق بسر المهنة وغيرها من الأحكام المشار إليها إلا ما اُستثني بنص قانوني.

---

(1) قضي في أمريكا بأنه إذا قامت إحدى الجامعات بضبط صور مخلة بالحياء في كمبيوتر أحد الأساتذة، فإن هذا الضبط يتفق مع صحيح القانون، حيث لا يتوافر لدى صاحب الجهاز في هذه الحالة موقع مقبول لاحترام الحياة الخاصة، وان تفتيش الرئيس الإداري للكمبيوتر يتفق مع صحيح القانون. مشار إليه لدى شيماء عبد الغني محمد عطا الله، مرجع سابق، ص76.

(2) قضي في فرنسا بإدانة مدير إحدى دور الشباب لقيامة بوضع جهاز تسجيل للمكالمات التي تتم من قبل العاملين بالدار التي يشرف عليها، لكي يقوم بقطع المكلمات التي تجري خارج نطاق العمل، بعد ملاحظته زيادة في فواتير الهاتف، ذلك أنه ليس من حقه أن يقوم بتسجيل المكالمات الخاصة بالعاملين والنزلاء في الدار والمستخدمين لا جهزنها. مشار إليه لدى شيماء عبد الغني محمد عطا الله، مرجع سابق، ص81.

(3) راجع: المواد (146 و 148) إ. ج. ي .

وبالنسبة لقانون الإجراءات الجزائية الجزائري بتعديلاته السابقة فلم يتضمن أي حكم في مسألة الرقابة والتصنت على المحادثات التلفونية، كما لم يوجد في قضاء المحكمة العليا ما يفيد بأن هذه المسألة قد أثيرت أمامها[1]. إلا أنه من خلال التعديل الأخير ل ق.أ.ج.ج ديسمبر 2006، يلاحظ بأنه قد تم استحداث نصوص قانونية تتضمن عدد من الأحكام [2] منها:

- وضع الترتيبات التقنية من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.
- يمكن القيام بوضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج مواعيد التفتيش والضبط المحددة في القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.
- عدم المساس بالسر المهني بالنسبة للأماكن التي يشغلها أشخاص مكلفون بالمحافظة على أسرار الآخرين.
- اكتشاف جرائم أخرى بصورة عارضة لا يكون سببا في بطلان الإجراءات.
- أن يشمل الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابر ومدتها.
- تكون أقصى مدة للأذن أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق.
- يجوز لوكيل الجمهورية أو قاضي التحقيق أو ضابط الشرطة القضائية المأذون له أو المناب، تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالموصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية المشار إليها في الفقرة الأولى.

---

(1) أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص95.
(2) راجع المواد (من 65 مكرر 5 إلى 65 مكرر 10) إ.ج. ج رقم (22- 06) المؤرخ في 20 ديسمبر 2006.(ج.ر 84.ص8)

- تحرير محضر عن كل عملية اعتراض أو تسجيل للمراسلات، وكذلك عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت، والتسجيل الصوتي والسمعي والبصري، ويذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.
- نسخ وإيداع المراسلات والصور والمحادثات المسجلة المفيدة في إظهار الحقيقة في محضر يودع في بالملف.
- ترجمة المكالمات الأجنبية بعد نسخها بمساعدة مترجم يسخر لهذا الغرض.

ومن خلال الأحكام السابقة يمكن الخروج بأن ق. إ.ج.ج قد تميز عن ق.إ.ج.ي بالنص على الرقابة التقنية على المحادثات ولم يجعلها تقتصر على المحادثات الهاتفية وإنما على الكلام المتفوه بشكل عام، مما يجعل النص قابلا للتطبيق على جميع المحادثات بغض النظر عن الوسيلة المستخدمة، كما أن الألفاظ التي استخدمت في نصوص القانون الجزائري قد شملت ألفاظا ذات طبيعة تقنية في مجال الرقابة الإلكترونية ومنها لفظ الالتقاط والاعتراض، وجعل تطبيق تلك الأحكام مقتصرا على حالة الضرورة في التحري في الجريمة المتلبس بها، أو التحقيق في عدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويكون ذلك بموجب إذن من وكيل الجمهورية.

ولكون تلك الأحكام لم تشر بنص صريح إلى الرقابة على الاتصالات الإلكترونية فقد ضمنها المشرع الجزائري في القانون رقم(09- 04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما في الفصل الثاني منه تحت عنوان مراقبة الاتصالات الالكترونية، عن طريق وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع محتواها في حينها، وقد شملت على نوعين من الرقابة، الأولى: وقائية غرضها الوقاية من الجرائم الخطرة المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

---

(1) تضمنت الفقرتان(أ، ب) من المادة (4) من القانون رقم (09-04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، الحالات التي يتاح من خلالها إجراء الرقابة الإلكترونية، للوقاية من تلك الجرائم، وتشمل تلك الحالات على : الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وفي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

والثانية وهي المقصودة في هذا الموضع غرضها ضبطي وقضائي وتشمل حالتين:

الأولى: لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تلك المراقبة.

الثانية: في إطار طلبات المساعدة القضائية الدولية المتبادلة (1).

ومع أن القانون اليمني لم يتضمن مثل تلك النصوص، فلا يوجد ما يمنع من إمكانية تطبيق النصوص التقليدية في ق. إ. ج. ي على الاطلاع وضبط الرسائل الإلكترونية، ومراقبة شبكات الحاسوب والانترنت للتشابه الكبير بين الرسائل والمحادثات سواء كانت تقليدية أم الكترونية، إلا أنه يفضل إضافة عبارة الرسائل الإلكترونية وشبكات الحاسوب والإنترنت، ووضع الترتيبات التقنية التي تساعد على عملية الرقابة إلى النصوص القانونية التي تنظم ضبط ومراقبة الرسائل والمحادثات الهاتفية، أسوة بالتشريع الجزائري، وقوانين العديد من الدول (2).

ليصبح نص المادة (148) إ.ج.ي على النحو التالي(للنيابة العامة أن تأمر بضبط جميع الخطابات والرسائل والصحف والمطبوعات لدى مكتب البرق والرسائل الإلكترونية لد مزودي خدمات الإنترنت، وأن تأمر بمراقبة المحادثات السلكية واللاسلكية، وكذلك شبكات الحاسوب والإنترنت، وإجراء تسجيل الأحاديث التي تجري في مكان خاص، ويمكنها في سبيل ذلك وضع الترتيبات التقنية لمراقبتها وتسجيل محتواها متى كان ذلك لازما لكشف الجريمة وفي جميع الأحوال يكون الأمر مسببا ولمدة لا تزيد عن ثلاثين يوم).

مع إحاطة ذلك بالضمانات اللازمة للحفاظ على الحقوق المتعلقة بالحماية الخاصة للأفراد، ومنها المحافظة على أسرارهم ، وعدم المساس بالسر المهني أثناء القيام بتلك الإجراءات وغيرها من الضمانات الكفيلة بالحفاظ على حقوق وحريات الأفراد.

---

(1) الفقرتان (ج.د) من المادة (4) من القانون رقم (09-04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما.

(2) ومن تلك الدول التي تضمنت في تشريعاتها النص على مراقبة والاعتراض على الاتصالات الإلكترونية وسماعها فرنسا من خلال القانون الصادر في 10 يوليو 1991، وفي هولندا نص القانون على (أنه يجوز لقاضي التحقيق أن يأمر بالتصنت على شبكة اتصالات الحاسوب في حالة أن يكون هناك جريمة خطيرة ضالع فيها المتهم، وفي أمريكا فإنه يجوز اعتراض اتصالات الحاسب الآلي بشرط الحصول على إذن تفتيش صادر من القاضي.راجع: هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص222.

المطلب الرابع

إجراء الخبرة لاكتشاف الجرائم المعلوماتية

إن ضرورة استعانة المحقق أو القاضي بالخبير في مجال الجرائم المعلوماتية، يكاد يكون ضرورة لا يمكن الاستغناء عنها، نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة غير المادية لمحل الاعتداء[1].

ومع أهمية الخبرة وضرورياتها في مجال كشف الجرائم المعلوماتية وضبط الأدلة المترتبة عليها، إلا أنها لا تخلو من المشكلات التي تعيق إجراء التحقيق بدلا من تسهيل القيام به، فما هي تلك المشكلات؟ وهل تفي النصوص القانونية في القانون اليمني والجزائري المتعلقة بالخبرة في معالجة تلك المشكلات؟

1- تعيين الخبير

إن أهم مشكلة تواجه نظم الخبرة عامة تتمثل في تكوين الخبير الذي سيتم الاستعانة به، ذلك أن الاستعانة بالخبرة في مجال تكنولوجيا المعلومات لا يعتمد على شهادة خبير تتوافر فيه الشروط الشكلية والموضوعية التقليدية المتطلبة بالخبير وإنما خرجت عن ذلك، وتطلب الأمر ضرورة توافر شروط أخرى تتناسب والتطور الحادث في تكنولوجيا المعلومات والجرائم الواقعة عليها [2].

كما أن اختيار الخبير في الجرائم التي تقع في مجال تكنولوجيا المعلومات يتحدد تبعا لنوعية الجريمة المرتكبة وأنواع الحاسبات والشبكات والبرامج المستخدمة فيها، وقد لا يوجد خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها وشبكاتها، كما لا

---

(1) يتطلب للخبير في مجال كشف الجرائم المعلوماتية أن يكون لديه الإلمام الكافي في الجوانب التقنية والفنية والتي منها:

- المعرفة بتركيبات الحاسبات وصناعتها وطرازها، ونوع نظم التشغيل، والأنظمة الفرعية المستخدمة، بالإضافة إلى الأجهزة الطرفية الملحقة وكلمات المرور، ونظم التشفير.
- طبيعة بيئة الحاسوب والشبكة من حيث تنظيم، ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردد موجات البث وأمكنة اختزانها.
- المواضع الرقمية المحتمل تواجد أدلة لإثبات فيها والشكل أو لهيئة التي تكون عليها.
- الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف الأدلة أو تغييرها أو إلحاق ضرر بالأجهزة.
- الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون إتلافها.
- عملية الربط بين الأدلة بشكلها الرقمي، ووضعها بعد أن يتم تخزينها بأوعية مادية، أو استخراجها بصورة مطبوعات يمكن للقاضي أن يفهمها ويستوعبها. لمزيد من التفصيل راجع: عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، مرجع سابق، ص394، ص395.

(2) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص1034.

يوجد خبير قادر على التعامل مع أنواع الجرائم التي تقع عليها، أو ترتكب بواسطتها[1]. وبدلا من أن تستفيد جهة تحقيق العدالة من الخبير، فقد يكون سببا في فقدان الأدلة، بسبب عدم التخصص الدقيق في المسألة التي تحتاج إلى خبرة، وقد تحتاج إلى أكثر من خبير.

وقد يتم إتلاف الأدلة بسبب خطأ مشترك بين الخبراء والجهة المجني عليها، ومثال ذلك ما حدث في تحقيق إحدى الجرائم المعلوماتية والتي تدور وقائعها حول قيام أحد الأشخاص في إحدى الشركات، بوضع قنبلة منطقية بنظام حاسبها الآلي، تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيرا للتحقق من صحة ذلك، وإبطال مفعول القنبلة إن وجدت، وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من البرنامج الموضوعة فيه، وعندما تولت الشرطة التحقيق اتضح أنه بإزالة القنبلة أتلفت كل الأدلة على وجودها[2].

ومشكلة الخبرة في مجال التكنولوجيا الرقمية لا تقتصر على النظم التي تعتمد على الخبراء المقيدين في الجداول القضائية- النظم الفرانكفونية- حيث تواجه مشكلة عدم وجود أو كفاية الخبرات الفنية والتقنية ذات العلاقة بالجوانب الرقمية في مسائل معينة معروضة على الجهات القضائية في تلك الجداول، بل إنها تشمل النظم التي لا تعترف بوجود فكرة جداول الخبرة القضائية- النظم الانجلوفونية- فهي وإن بدأت في الاستعانة بفكرة الاستعانة بجداول الخبراء في المحكمة كفكرة جديدة، إلا أن ذلك ذالك سوف يجعل الخبرة التقنية في مجال الإنترنت على ذات المنوال التي هي عليه من مشاكل سيما في إطار تصنيف الخبرة[3].

كما أن دخول ما يسمى بالخبرة الخاصة والتي تستمد قوتها من المنافسة القوية بين المنظمات الخاصة، والتي بموجبها قد يتم الاستعانة بخبير في مجال التكنولوجيا الرقمية في الأمور التي يرى المحقق عرضها عليه، بهدف كشف غموض الجريمة لما يتمتع به هؤلاء الخبراء من تخصصات دقيقة في مجال التقنية الرقمية، فحتى هذا النوع من

([1]) هشام محمد فريد رستم، أصول التحقيق في جرائم الحاسب الآلي، مرجع سابق، ص433، عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر،2004، ص97.

([2]) حسين بن سعيد سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، بحث منشور على شبكة الإنترنت، على موقع المنشاوي، ت.د 2009/4/5 على الرابط:
http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014

([3]) راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص1033، ص1034.

الخبرة فإنه لا يخلو من المشكلات التي قد لا تعيق إجراءات التحقيق فحسب، بل إنها قد تكون سببا في بطلان الإجراء في حالة الدفع بذلك، ذلك أن بعض القوانين تخول للمتهم الاستعانة بخبير استشاري، ولا تخول ذلك لسلطة التحقيق أو الاتهام، حيث يكون بإمكانهم الاستعانة بخبير من الخبراء المنصوص عليه في الجدول القضائي، وقد لا يجد المحقق خبيراً في المجال الرقمي في ذلك الجدول، وذلك ما يستدعي التدخل في مجال الخبرة الاستشارية بنصوص قانونية يسمح بموجبها الاستعانة بالخبرة الاستشارية الرقمية الكاملة دون التقيد بخبراء الجدول المعتمدين(1). أسوة بدول متقدمة في مجال التكنولوجيا الرقمية لم تقتصر في مجال الخبرة على الخبرة الوطنية بل إنها قد تستعين بخبرة أجنبية (2).

وحتى في حال قبول العمل بالخبرة الاستشارية، أو الخبرة من خارج الجدول القضائي(3)، فإن نقص خبرة المحقق أو القاضي في مجال التكنولوجيا الرقمية سيترتب عليه عدم استطاعة أي منهم تحديد دور الخبير المعلوماتي في المسألة المنتدب بشأنها على وجه الدقة، حيث تعرض مبدأ القاضي خبير الخبراء لهزات عنيفة في ظل التطور العلمي التقني، والذي قد لا تغني في فهمه والرقابة عليه الإلمام بالجوانب النظرية والقانونية، وبالتالي فإن الخبير سيحل محل أي منهم في تحديد مهمته بنفسه، بل إنه من الناحية الواقعية سيكون هو المحقق وهو القاضي.

ولا يمكن تخطي هذه المشكلة دون تدريب تخصصي يراعي فيه العناصر الشخصية للمتدربين، من حيث توافر الصلاحية العلمية، والقدرات الذهنية والنفسية لتلقي التدريب، ويكون من الأسهل تدريب متخصصين في تكنولوجيا المعلومات وشبكات

---

(1) راجع : عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص892.

(2) من الدول التي فعلت الاستعانة بالخبير الاستشاري، و الاعتراف بالخبرة الأجنبية أمام القضاء الوطني في مجال الإجرام المعلوماتي فرنسا، حيث تستعين بخبيرين أحدهما انجليزي والآخر أميركي في القضايا التي تحتاج إلى خبرة أجنبية، كما استعان القضاء الفرنسي في عدد من القضايا منها قضية اتحاد الطلاب اليهود، وقضية منظمة ليكراء ضد شركة ياهو بخبراء من خارج الجدول، ومن خارج فرنسا لكي يضعوا رأيا فنيا يتعلق بإمكانية الفلترة والتصفية عبر الإنترنت. راجع حسين بن سعيد بن سيف ألغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مرجع سابق، على الرابط:
http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014
وراجع أيضا:عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق ص1035.

(3) يعد قانون الإجراءات الجزائية اليمني من القوانين التي لم تلزم المحقق أو القاضي باختيار خبير من الخبراء المحددين في الجدول القضائي، وترك مسألة التحديد تبعا للحاجة.راجع: المواد (من207- 216،و243) إ.ج.ي، أما قانون الإجراءات الجزائية الجزائري فقد ألزم جهات التحقيق والحكم بانتداب خبير من الخبراء المقيد في الجدول القضائي، واستثناء من ذلك اختيار خبير من خارج الجدول وفق قرار مسبب بذلك.راجع: المادة(144) إ.ج.ج.وبشأن الخبرة بشكل عام . راجع (المواد من 143 - 156)إ.ج.ج.

الاتصال من رجال الشرطة، أو ممثلي الإدعاء العام، على أن تكون خبرة المتدرب حسب ما يرى البعض مدة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة، وتصميم النظم وتحليلها، وإدارة الشبكات وعمليات الحاسب الآلي [1].

2- مدى كفاية النصوص التقليدية في معالجة المشكلات المتعلقة بالخبرة المعلوماتية

لبيان دور القانون اليمني والجزائري في مجال الخبرة الرقمية لابد من التعرض للنصوص القانونية ذات العلاقة بالخبرة في كلا القانونين.

وبهذا الخصوص فقد نظم ق. إ. ج. ي الأحكام المتعلقة بالخبرة من خلال المواد (من 207 إلى216)، كما نظمها ق. إ.ج. ج في المواد(من 143 إلى 156)[2]، حيث تضمنت تلك المواد عدد من الأحكام المتعلقة بالخبرة سوف نشير إلى أهمها مع بيان أوجه الاختلاف أن وجدت وهي:

- يكون حق الاستعانة بخبير في القانون اليمني في أي مسألة متعلقة بالتحقيق من عدمه للنيابة العامة، حسب تقديرها، وتكون وجوبيه عندما يتطلب الأمر بيان سبب الوفاة وطبيعة الإصابة الجسمانية، أو تحديد الحالة النفسية للمتهم أو الشاهد في حالة الشك، أو لبيان سن المتهم أو المجني عليه إذا تطب التحقيق ذلك[3].

بينما يكون الحق في الاستعانة بخبير أو أكثر في القانون الجزائري لقاضي التحقيق أو الجهة المخولة بالحكم، وذلك في المسألة أو المسائل التي تحتاج إلى خبرة، ويتم اختيار الخبير من قائمة الخبراء المحددين بجدول المجلس القضائي، ويستثنى اختيار خبير من غير المعتمدين بقرار مسبب[4].

-يوجب القانون اليمني حضور المحقق أعمال الخبرة وإبداء ملاحظته، إلا إذا اقتضى الأمر إثبات الحالة بدون حضوره نظرا لضرورة القيام ببعض أعمال تحضيرية أو تجارب متكررة أو لأي سبب آخر[5].

([1]) هشام محمد فريد رستم، أصول التحقيق الجنائي الفني في الجرائم المعلوماتية، مرجع سابق، ص 496.

(2) راجع: المواد (من 207 إلى 216) من القانون اليمني رقم (13) لسنة 1994 بشأن الإجراءات الجزائية، وكذلك المواد (من 143 إلى 156) من القانون رقم (22-06) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري (ج.ر 84).

([3]) رجع: المادة (207) والمادة(208) إ.ج. ي.

(4) راجع: المادة(143) إ. ج.ج.

(5) المادة (207) إ.ج. ي.

بينما لم يتضمن القانون الجزائري شرط الحضور بنص صريح، إلا انه من ناحية أخرى يخضع الخبراء في مهامهم لسلطة قاضي التحقيق أو الجهة التي أمرت بإجراء الخبرة، وذلك ما يوحي بأن حضور قاضي التحقيق مسألة جوازيه وليست وجوبيه، لذلك فإنه يتطلب من عضو النيابة العامة ومن قاضي التحقيق الإلمام بالأمور الفنية، أو على الأقل الإطلاع عليها، حيث يرجع قصور قضاة التحقيق في الأداء إلى عدم التخصص ونقص الخبرة، والتجربة (1)، وإذا كان ذلك الرأي في المسائل التي ليست لها علاقة بتكنولوجيا المعلومات، فإن الأمر سيكون أكثر تعقيدا عند تطلب الخبرة في مجال تكنولوجيا المعلومات في ظل نقص الخبرة لدى جهات التحقيق أوالحكم.

-وفقا للقانون اليمني فإنه يجب على الأطباء والخبراء الذين يكلفون بأعمال الخبرة أن يحلفوا أمام المحقق اليمين القانونية قبل مباشرتهم العمل ما لم يكونوا قد أدوها بحكم وظائفهم. مادة(207) إ.ج.ي.

أما في القانون الجزائري فيكون أداء اليمين بالنسبة للخبير المقيد في الجدول مرة واحدة عند تقييده، بينما يلزم الخبير المعين من خارج الجدول أداء اليمين لكل مهمة محددة بذاتها. مادة (145) إ. ج. ج.

- يكون للخصوم بموجب القانون اليمني رد الخبير إذا وجدت أسباب قوية بموجب طلب يقدم إلى النيابة العامة للفصل فيه خلال ثلاثة أيام، ويجب أن يبين فيه أسباب الرد ويترتب على هذا الطلب عدم استمرار الخبير في عمله إلا في حالة الاستعجال بأمر من النيابة العامة. مادة (209) إ.ج.ي.

وبالمقابل فلم يتضمن القانون الجزائري ما يتعلق برد الخبرة بناء على طلب الخصوم، وإنما تضمن حكما أخر يتعلق بعدم قبول طلب الخبرة المقدم من النيابة العامة أو الخصوم، إذا رأت الجهة المخولة بالتحقيق أو الحكم بأن لا موجب لطلب الخبرة المقدم من الخصوم، أو من النيابة العامة، وعليها إصدار قرار مسبب بذلك في مدة أقصاها ثلاثون يوما، ولطرف المعني التظلم من القرار، وكذلك في حال عدم صدور

(1) أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص120.

قرار مسبب، عن طريق إخطار غرفة الاتهام خلال مدة عشرة أيام، وعليها الفصل في الطلب خلال ثلاثون يوما، ويكون قرارها غير قابل للطعن[1].

-للخصوم حسب القانون اليمني الاستعانة بخبير استشاري، وطلب تمكينه من الإطلاع على الأوراق وسائر ما سبق تقديمه للخبير المعين من قبل المحقق السابق على أن لا يترتب على ذلك تأخير السير في الدعوى. مادة (110) إ.ج. ي..

وهذا الحكم تضمنه القانون الجزائري ولم لم يطلق عليه خبير استشاري، وأُطلق عليه الخبير من خارج الجدول القضائي، والذي يتم انتدابه من قبل قاضي التحقيق بموجب طلب من النيابة العامة أو الخصوم، أو بدون طلب. مادة (144)إ. ج. ج.

-في القانون اليمني يقدم الخبير تقريره كتابة في الميعاد الذي يحدده عضو النيابة أو المحكمة، وفي حالة تعدد الخبراء ولم يصلوا إلى رأي مشترك يقدم كل منهم تقريرا منفصلا، وتقرير الخبير لا يكون ملزما للنيابة العامة أو المحكمة، إلا أن عدم الموافقة على التقرير يجب أن تكون مسببه، كما يجوز طلب تقرير أضافي من الخبير نفسه أو من خبير أخر إذا احتوى التقرير الأول على أوجه نقص، كما يجوز أيضا طلب تقرير جديد من خبير آخر إذا ثار شك حول صحة التقرير الأول[2].

ولم يتضمن القانون الجزائري حق المحقق في طلب تقرير جديد من خبير أخر، أو تقرير إضافي من نفس الخبير، إلا أنه قد تم معالجة هذه المسألة بتمكين الخبير من الاستعانة بفنيين من أصحاب الاختصاص إذا تطلب الأمر ذلك بموجب طلب يقدمه لقاضي التحقيق، ويعينوا بأسماؤهم ويؤدون اليمين، ويرفق تقريرهم بتقرير الخبرة[3].

كما عالج المسألة من ناحية ثانية، بأن أوجب على قاضي التحقيق استدعاء من يعنيهم الأمر من أطراف الخصومة، وإحاطتهم بما انتهت إليه تقارير الخبرة من نتائج، وعليه تلقي أقوالهم بشأنها وتحديد موعد لإبداء ملاحظاتهم عليها، أو تقديم طلبات لاسيما فيما يخص إجراء خبرة تكميلية، وعليه أن يبت في حال رفض تلك الطلبات خلال مدة

---

(1) راجع: الفقرات (2، 3 من المادة 143) من القانون رقم (22 - 06) المؤرخ في 20 ديسمبر 2006، حيث تضمنت هاتان الفقرتان المواعيد الخاصة بالبت في طلبات الخصوم - المتعلقة بإجراء خبرة تكميلية، أو الاعتراض على قرار الخبرة- من قبل قاضي التحقيق، ومن غرفة الاتهام، في حالة عدم البت في الموعد المحدد من قبل قاضي التحقيق، حيث لم تكن المادة ذاتها وفقا للأمر رقم (155- 66) المؤرخ في 8 نيو1966 تتضمن تلك المواعيد الزمنية.

(2) راجع: المادة (111) والمادة (116) إ.ج.ي رقم(13) لسنة 1994.

(3) راجع : المادة (149) إ. ج. ج.

ثلاثين يوما، وفي حالة عدم قيامه بذلك فإن للخصم إخطار غرفة الاتهام خلال مدة عشرة أيام، وعليها الفصل في ذلك خلال مدة ثلاثين يوما، ويكون قرارها غير قابل لأي طعن(1).

-يجوز وفقا للقانون اليمني أن يؤدي الخبير مهمته بغير حضور الإطراف، وله بغية التزود بإيضاحات أضافية لإعداد تقريره أن يطلب الإذن بالإطلاع على الأوراق وحضور سماع الشهود والمتهم وتوجيه أسئلة مباشرة لهم، كما يجوز أن توضع تحت تصرفه الأدلة المادية(2).

أما في القانون الجزائري فإن للخبير في سبيل القيام بمهامه والحصول على معلومات تفيده في مجال الخبرة في القضية التي كلف برفع تقرير خبرة بشأنها، الاستماع لكل شخص يرى ضرورة لسماعه، باستثناء المتهم الذي لا يحق للخبير الاستماع لأقواله، إلا بواسطة قاضي التحقيق وبحضوره فقط(3).

-يجب تحديد المدة التي يجب على الخبير أو الخبراء إنجاز المهام المناطة بهم خلالها، ويكون تحديد موعد تقديم التقرير من اختصاص عضو النيابة أو المحكمة(4).

ويجوز تمديدها وفقا للقانون الجزائر بقرار مسبب من قاضي التحقيق بناء على طلب من الخبير أو الخبراء، وعليهم إيداع تقاريرهم خلال تلك المدة، ما لم فمن حق الجهة التي انتدبتهم استبدالهم، وعليهم أن يقدموا نتائج أبحاثهم، وأن يردوا الأشياء التي سلمت لهم بهدف القيام بمهامهم، في ظرف ثمان وأربعين ساعة، ولا يكون ذلك حائلا دون مجازاتهم تأديبيا، والتي قد تصل إلى عقوبة الشطب من جدول الخبراء(5).

من خلال الأحكام المشار إليها يتضح بأن القانون اليمني قد أعطى الحق في الاستعانة بخبير للنيابة العامة، بينما أعطاها القانون الجزائري لقاضي التحقيق وتقتصر صلاحيات النيابة العامة على تقديم طلب الاستعانة بخبير لقاضي التحقيق.

---

(1) راجع المادة (154) معدله بالقانون رقم (22- 06) المؤرخ في 20 ديسمبر 2006، حيث لم تكن المادة نفسها قبل التعديل في ظل الأمر رقم (66- 155) المؤرخ في 8 يونيو 1966 تتضمن مواعيد البت في طلبات الخصوم من قبل قاضي التحقيق أو غرفة الاتهام.

(2)راجع: المادة (212) إ. ج.ي.

(3) المادة (151) إ. ج. ج.

(4) راجع: المادة (211) إ. ج. ي.

(5) راجع: المادة (148) إ.ج.ج.

كما يلاحظ أن القانون اليمني قد تضمن حالات يكون فيها الاستعانة بالخبرة وطلب التقارير الخاصة بها وجوبيا وفقا لما تم الإشارة إلى ذلك سابقا، ولم يتضمنها القانون الجزائري، حيث جعل حق الاستعانة بالخبير جوازيا، عدى الحالات التي يتم رد طلب الاستعانة بالخبير المقدم من النيابة العامة أو الخصوم إلى قاضي التحقيق في حالة الرفض، ويتم إخطار غرفة الاتهام حيث يكون قرارها غير قابلا للطعن.

كما أن القانون الجزائري قد تضمن مددا زمنية يتم من خلالها البت في طلب النيابة العامة أو الخصوم في تقرير الخبرة أو رده، وحددها ثلاثون يوما بالنسبة لقاضي التحقيق ومثلها بالنسبة لغرفة الاتهام في حال عدم البت في الطلب. وفي حالة تعدد الخبراء واختلافهم في وجهة النظر، أو أبداء تحفظات من قبل البعض على بعض النقاط، فإن القانون اليمني يلزم كلا منهم رفع تقرير مستقل، بينما في الجزائري يكتفي بتقرير واحد على أن يبدي كلا منهم تحفظاته.

ويلاحظ أخيرا بإمكانية تطبيق تلك الأحكام على الخبرة في مجال الجرائم المعلوماتية، حيث لا يوجد ما يمنع من تطبيقها، وتظل المشكلة المتعلقة بالخبرة مقتصرةً على عدم وجود نصوص قانونية تنظم ما يخص الخبرة الرقمية من وضع الترتيبات التقنية المسهلة لاتخاذ الإجراء، وكذلك نقص الخبراء في مجال التكنولوجيا الرقمية والجرائم الواقعة عليها، وعلى وجه الخصوص في الدول التي مازالت متخلفة في مجال التكنولوجيا الرقمية، في الوقت الذي أضحت التقنية الرقمية تتدخل في أغلب المعاملات، وبالتالي فلابد من الاهتمام في مجال التخصص التقني في شتى مجالات علوم التكنولوجيا الرقمية ومتابعة كل جديد في ظل التطور الحادث مابين الآونة والأخرى.

كذلك فإن نقص الخبرة لدى سلطات تحقيق العدالة تظل مشكلة أخرى حتى في ظل إمكانية تطبيق النصوص التقليدية عليها، فحضور المحقق أعمال الخبرة وإشرافه والرقابة عليها، وتحديد المواضيع التي تحتاج إلى الاستعانة بالخبرة في أمر ندب الخبير من الأمور الفنية التي تستلزم في المحقق أو القاضي أن يكون ملما بها، وهذا ما لم يتوافر في الدول المتخلفة في مجال التكنولوجيا الرقمية، وبالتالي فلابد من تدريب كوادر الأجهزة الضبطية والعدلية التدريب الكافي في مجال الخبرة الرقمية التي يستطيع من خلالها مأمور الضبط القضائي أو القاضي السيطرة على أعمال الخبرة أثناء التحقيق أو

المحاكمة إعمالا لقاعدة "القاضي خبير الخبراء"، وبهذا الشأن فقد قامت جمهورية الجزائر بإيفاد أعداد من الشرطة والدرك الوطني وغيرها من الأجهزة القائمة على تحقيق العدالة لتلقي التدريب في فرنسا وبلجيكا وكندا.

كما قامت قيادة الدرك بإنشاء مركز وقاية ومكافحة الإجرام المعلوماتي ببوشاوي[1]، وكذلك تم إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي بموجب المرسوم الرئاسي رقم (04- 432)المؤرخ في 20 ديسمبر 2004، وتم تنظيم المصالح والأقسام والمخابر لذات المعهد بموجب قرار وزاري مشترك مؤرخ في 14 ابريل 2007والذي تضمن ضمن مصالحه مصلحة الخبرات الخاصة بالدلائل التكنولوجية[2].

كما أن القسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية بالمديرية العامة للأمن الوطني ومصالحها في بعض الولايات يقدم الخبرة المتميزة في ذات المجال في القضايا ذات الطابع الرقمي، حيث يوجد به خبراء متخصصين في تحليل واستعادة البيانات المحذوفة وتتبع عنوان Ip، ومعالجة الصور ومطابقتها، ومعرفة الصور التي تم تركيبها، وكذلك الخبرة المتعلقة برسائل الهاتف الجوال.

كما أن المشرع الجزائري قد تنبه أخيرا وعمل على وضع النصوص القانونية ذات العلاقة بالخبرة الرقمية، ومن ذلك النص على إمكانية الاستعانة بكل من له دراية في عمل المنظومة المعلوماتية حيث ورد النص بأنه: (يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها)[3].

كما عمل على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وجعل من مهامها إنجاز الخبرات القضائية التي تحتاج إليها السلطات القضائية، ومصالح الشرطة القضائية، حيث ورد النص الذي يحدد المهام

---

(1) مقابلة أجرتها جريدة الشروق الجزائرية مع مسئولين في الدرك الوطني منشوره على موقعها على الرابط: http://www.echoroukonline.com/modules.php?name=News&file=article&sid=10731

(2) راجع القرار الوزاري المؤرخ في 14 ابريل 2007 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي.(ج.ر 36 ، 3يونيو 2007، من ص 14 –ص17)

(3) الفقرة الأخيرة من المادة (5) من القانون رقم (09 - 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (ج.ر 47، ص6).

المتعلقة بالخبرة بأن من مهام الهيئة (مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية) [1].

وعلى المشرع اليمني إدراج ما يتصل بالخبرة المعلوماتية ضمن التعديلات القادمة، حتى لا يمكن الطعن بالإجراءات ذات الطبع التقني التي تقوم بها السلطات المختصة بذلك بما فيه الترتيبات التقنية التي قد يقوم بها الخبراء في حالة الاستعانة بهم، والسماح لجهات تحقيق العدالة بالاستعانة بالمؤسسات المتخصصة في مجال الخبرة الرقمية، وكذلك الخبرات الأجنبية في حال تطلب الأمر ذلك، مع عدم إغفال تدريب كوادر متخصصة في مجال التحري والتحقيق والخبرة الرقمية سواء في الداخل أو الخارج.

([1]) الفقرة (ب) من المادة (13) من القانون رقم (09 - 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (ج.ر 47، ص8)

الفصل الثاني

الاختصاص القضائي والدليل الإلكتروني ودور التعاون الدولي

لقد أضحى سائدا في ظل التطور التكنولوجي بأن جرائم المعلوماتية لا تتقيد بنطاق جغرافي معين، فقد ترتكب في أكثر من نطاق اختصاص على إقليم الدولة الواحدة، وقد ترتكب في أكثر من دولة، مما يثير تنازع الاختصاص القضائي داخليا وخارجيا، ولذلك فإن الدول المتقدمة في مجال التكنولوجيا الرقمية، هي دائما السباقة في مواجهة ذلك النوع من الجرائم بقوانين مستحدثة، حيث أن بعض القوانين التي سيتم الإشارة إليها تخول للسلطات في ذات الدولة حق الدخول وتفتيش أنظمة الغير خارج نطاق الاختصاص متجاهلة الاعتداء على سيادة الدول، كما أن تفوق تلك الدول بالجانب التكنولوجي، أو الرقمي، وعلى وجه الخصوص الجانب الفني قد يجعلها تقوم بالرقابة، وتفتيش أنظمة الغير دون إذن أو تنسيق مع تلك البلدان.

إضافة إلى أن ظهور نوع جديد من الأدلة ذات الطابع المعنوي وليس المادي، سهلة الإخفاء والتغيير، تتطلب من الجهات القائمة على تحقيق العدالة التعامل معها بحذر وبأسلوب فني تقني، حفاظا عليها من الضياع، هذا النوع من الأدلة تثير العديد من المشاكل التي تتعلق بصعوبة التعامل معها، وكشفها وضبطها، وحفظها.

بل أن تلك الأدلة قد أضحت محل نظر في مدى حجيتها في الإثبات، لكون الفقه والقضاء والتشريعات كانت تعتمد على الدليل المادي الملموس، وأصبحت مضطرة للتعامل مع نوع جديد من الأدلة، ليست ملموسة أو محسوسة، فهي عبارة عن موجات كهرومغناطيسية.

ولوضع معالجات وحلول للمشاكل الإجرائية للجرائم المعلوماتية، فقد تم عقد العديد من المؤتمرات، وتوقيع العديد من الاتفاقيات والتي أهمها اتفاقية بودابست لمكافحة الإجرام المعلوماتي، كما أضحت الحاجة ماسة للتعاون الدولي لما له من دور في معالجة تلك المشكلات، لما تم ذكره فسوف نتناول المشكلات التي تتعلق بالاختصاص القضائي والدليل الالكتروني في المبحث الأول من هذا الفصل ، ونبين دور الاتفاقيات والتعاون الدولي في مكافحة تلك الجرائم في المبحث الثاني.

المبحث الأول

الاختصاص القضائي والدليل الإلكتروني

يتزامن مع ظهور الجرائم المعلوماتية العديد من المشكلات الخاصة بتحديد القانون الواجب التطبيق، والقضاء المختص بنظر تلك الجرائم، سواء على النطاق الداخلي أو النطاق الخارجي، فالإنترنت لا يعترف بوجود حدود بين الدول، إذ لا يحتاج المجرم إلى الحركة من مكانه الذي يقبع فيه في إحدى غرف منزله أمام جهاز الحاسوب، إذ يستطيع أن يرتكب جريمته في بضع ثوانٍ ، بداية من مكان تواجده وارتكاب أفعاله ذات الطابع المعنوي، وتحقيق نتائج تلك الأفعال في أكثر من دولة، وخاصة الجرائم التي ترتكب بواسطة الفيروسات، حيث تشكل الشبكة بأجهزتها وبرامجها ومستخدميها مجتمعا فضائيا افتراضيا، كان هذا المجتمع الافتراضي سببا في وجود واقع افتراضي، يتمثل بالمكان الذي يعيش فيه مستخدمو الإنترنت مع المعلومات والأفكار وباقي مواد الإنترنت الذي يبدو كأنه يعلو كل أقاليم الدول، حيث لا يتقيد بحدود جغرافية أو سياسية [1].

كما برزت العديد من المشكلات التي تتعلق بالدليل الإلكتروني، سواء عادت إلى طبيعة الدليل ذاته، أو إلى حجيته في الإثبات، فقد ترتب على التطور المتزايد في استخدام الحاسوب وشبكة المعلوماتية، وما رافق ذلك من ظهور نوعية جديدة من الجرائم المعلوماتية، أن تغيرت أدلة تلك الجرائم من أدلة مادية ملموسة، سهلة المتابعة والكشف والإحراز، إلى أدلة معنوية سهلة الإخفاء والتعديل والتلاعب، تتحكم فيها بيانات وبرامج، وأضحى من المتطلبات الهامة في مجال عمل السلطات القضائية أن تتعامل مع تلك الأشكال المستحدثة من الأدلة في مجال الإثبات الجنائي تتناسب والتعامل مع تلك الجرائم ومقترفيها[2].

---

(1) أحمد عبد الكريم سلامة، الإنترنت والقانون الدولي الخاص، بحث مقدم إلى مؤتمر القانون والإنترنت، الذي انعقد بجامعة الإمارات العربية المتحدة من 1-3مايو 2000،ج3،ط3 ،2004، ص38. وراجع فهد سلطان محمد أحمد بن سليمان، مرجع سابق، ص28.

(2) تميزت الجرائم المعلوماتية عن التقليدية في العديد من الأمور منها حداثتها وظهورها بظهور التكنولوجيا الرقمية، واعتمادها على كيانات معنوية – موجات كهرومغناطيسية – في ارتكابها، كما تميز المجرم المعلوماتي عن التقليدي بالذكاء والاعتماد على جانب التفكير في ارتكاب الجريمة لا القوة العضلية كما في أغلب التقليدية، إضافة إلى الإلمام بالجوانب الفنية والتقنية، بل والتخصص في بعض الجرائم الهامة التي لا يرتكبها إلا فنيون ومتخصصون في مجال علوم الحاسوب والشبكات والبرامج، لذلك فإن لدى المجرم قدرة على إخفاء جريمته والتلاعب بالأدلة التي يمكن أن تترتب عليها، لذا فقد أصبح لزاما على السلطات القضائية أن تتعامل مع تلك الجرائم بما يتناسب معها من أدلة الكترونية .

المطلب الأول

الاختصـاص القضــائي

تعد الجرائم المعلوماتية وعلى وجه الخصوص المتعلقة منها بالإنترنت، من الجرائم التي تثير مسألة الاختصاص القضائي على المستوى المحلي أو الدولي.

وتثار مشكلة الاختصاص القضائي على المستوى الوطني أو الدولي، بحيث يمكن القول بأن مشكلة الاختصاص المحلي في الجرائم المعلوماتية تعني تنازع الاختصاص بين أكثر من جهة قضائية داخل إقليم الدولة، أما مشكلة الاختصاص الدولي فتعني تنازع الاختصاص بين أكثر من دولة.

1- الاختصاص القضائي الداخلي

يطلق على هذا النوع من الاختصاص بالاختصاص الداخلي أو الإقليمي، باعتبار أن القضاء الوطني هو المختص في الفصل في الدعوى الجزائية دون منازع، وهو يقوم على تحديد إطار جغرافي، أو دائرة اختصاص مكاني تتحدد بمنطقة معينة من إقليم الدولة، ويقوم هذا التقسيم على معايير ثلاثة هي: مكان وقوع الجريمة، أو مكان إقامة المتهم، أو مكان القبض على المتهم[1].

وبهذا الخصوص فقد نصت المادة(115) إ. ج. ي على تحديد اختصاص أعضاء النيابة العامة في التحقيق بالجرائم الواقعة في نطاق اختصاص المحاكم التي يعملون بها.

كما نصت المادة (234) من ذات القانون على الاختصاص المحلي بقولها (يتعين الاختصاص محليا بالمكان الذي وقعت فيه الجريمة، أو المكان الذي يقيم فيه المتهم، أو المكان الذي يقبض عليه فيه، ويثبت الاختصاص للمحكمة التي رفعت إليها الدعوى أولا، وفي حالة الشروع تعد الجريمة مرتكبه في كل محل وقع فيه عمل من أعمال البدء في التنفيذ)[2].

ونصت على ذات الاختصاص المادة(37) إ. ج.ج. بقولها (يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في

([1]) حسني الجندي، مرجع سابق، ص687.

([2]) راجع: المادة (115) والمادة (234)إ. ج. ي. رقم (13) لسنة 1994.

مساهمتهم فيها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى لو حصل هذا القبض لسبب آخر) [1].

كما نصت المادة (329) (تختص محليا بالنظر في الجنحة محكمة محل الجريمة، أو محل إقامة أحد المتهمين أو شركائهم، أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر) [2].

ومن خلال النصوص السابقة يتضح بأن الاختصاص القضائي المكاني يتطلب توافر حالة من الحالات الثلاث التالية:

أ- أن تكون الجريمة قد اقترفت بكاملها، أو أحد عناصر الركن المادي لها، أو تحقق صورة من صور الاستمرار بالنسبة للجريمة المستمرة، أو أي فعل من أفعال الاعتياد أو التتابع بالنسبة للجريمة المركبة، أو أي عمل من أعمال البدء في التنفيذ بالنسبة للشروع، في دائرة الاختصاص المكاني لعضو النيابة العامة أو قاضي التحقيق[3].

ب- أن تكون إقامة المتهم أو المشتبه به، أو إقامة أحد المشتبه بهم في دائرة اختصاص عضو النيابة العامة أو قاضي التحقيق، ويتحدد مكان الإقامة بوقت إتيان الجريمة.

ج- أ ن يكون قد القي القبض على أحد المتهمين أو المشتبه بهم في نطاق تلك الدائرة.

وتثار مشكلة الاختصاص القضائي المحلي بالنسبة لجرائم المعلوماتية، في حالة أن تكون الجريمة مرتكبة في أكثر من نطاق اختصاص محلي داخل الإقليم الوطني للدولة.

كما تثار المشكلة في حالة أن تكون الجريمة مرتكبة كلها على إقليم الدولة، بحيث لا يوجد قضاء أو قانون لدولة أخرى ينازع قوانين تلك الدولة، أو اختصاصها القضائي.

فالمشكلة إذن تتعلق بالاختصاص القضائي المحلي في حالة أن تكون الجريمة قد

---

(1) الفقرة (1) من المادة (37) من الأمر رقم (66 -155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية، وقد ظلت هذه الفقرة كما عليه في التعديلات التي كان أخرها في 2006، وأضيفت فقرة إليها تتعلق بتمديد اختصاص وكيل الجمهورية إلى نطاق محاكم أخرى في جرائم محددة.بموجب القانون رقم (04-14) المؤرخ في 10 نوفمبر 2004.

(2) الفقرة (1) من المادة (329) من القانون رقم (04-14)المؤرخ في 10 نوفمبر 2004 (ج.ر 71ص6)

(3) عبد الله أوهايبية، مرجع سابق، ص 324.

ارتكبت بكاملها في نطاق الإقليم الوطني، إلا أنها في أكثر من نطاق اختصاص قضائي داخل الدولة، بسبب طبيعة الجريمة وشبكة المعلوماتية، فالجريمة في هذه الفرضية سواء تمثلت بجريمة الدخول أم إتلاف بيانات الحاسوب، أو أنظمة المعالجة الآلية للمعطيات، وغيرها، قد ارتكبت بكامل أركانها في نطاق اختصاص المحاكم اليمنية أو الجزائرية، وهذه المشكلة يمكن القضاء عليها، في حال أن يتم تمديد الاختصاص القضائي داخل إقليم الدولة بما يتناسب وطبيعة الجريمة المرتكبة، حيث يكون بإمكان أي دولة وضع أو تعديل النصوص القانونية الإجرائية التي تنظم الاختصاص القضائي فيها بما يتناسب مع كشف وضبط تلك الجرائم وملاحقة مرتكبيها.

فكما أن الاختصاص القضائي وفقا للقواعد التقليدية في أغلب القوانين، ومنها النصوص سالفة الذكر في القانون اليمني والجزائري، ينعقد إما لمكان ارتكاب الجريمة، أو محل إقامة المتهم، أو مكان ضبطه، فهو كذلك في الجرائم المعلوماتية، إذ يمكن تطبيق أي قاعدة من قواعد الاختصاص المشار إليها سواءً تمثلت بمكان وقوع الجريمة، أم بمحل إقامة المتهم أو المشتبه به، أو مكان القبض عليه.

وينعقد الاختصاص وفقا لمعيار من المعايير المشار إليها بحسب السبق للمحكمة التي دخلت الدعوى الجزائية حوزتها قبل غيرها، فإذا نظرت القضية محكمة محل إقامة المتهم فإنها بالتالي تكون هي المختصة دون غيرها، ويكون من حقها تمديد اختصاصها بشأن اتخاذ أي إجراء من إجراءات المحاكمة، بشرط أن يكون ذلك التمديد بموجب نص قانوني، وذلك ما جعل القانون الجزائري يتميز عن اليمني في هذه المسألة، حيث مدد الاختصاص القضائي بالنسبة لعدد من الجرائم منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وجرائم الإرهاب، والمخدرات وغيرها مما نصت عليها المادة(37) والمادة (47) والمادة(80) والمادة (329) [1].

حيث نصت المادة(37- 2) على أن: (يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف).

([1]) راجع الفقر(2) من المادة (37)، والفقرة (4) من المادة (47) والمادة (80)، والفقرة (3) من المادة (329) من ق. إ. ج رقم (06 - 22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية.

ونصت المادة (47 -4) على : (عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضابط الشرطة القضائية المختص بذلك)(1).

كما نصت المادة(80) إ. ج. ج على جواز تمديد اختصاص قاضي التحقيق ليشمل المحاكم المجاورة لدائرة اختصاصه بقولها (يجوز لقاضي التحقيق أن ينتقل صحبة كاتبة بعد إخطار وكيل الجمهورية بمحكمته إلى دوائر اختصاص المحاكم المجاورة للدائرة التي يباشر فيها وظيفته، للقيام بجميع إجراءات التحقيق إذا ما استلزمت ضرورات التحقيق أن يقوم بذلك، على أن يخطر مقدما وكيل الجمهورية بالمحكمة التي سينتقل إلى دائرتها وينوه في محضره إلى الأسباب التي دعت إلى انتقاله).

كذلك نصت المادة(329) على: (يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف).

وبالتالي فإن التشريع الجزائري قد حسم المشكلة بالنسبة لتنازع الاختصاص القضائي بين الجهات القضائية الكائنة داخل الإقليم الوطني للدولة وهو اختصاص يتحدد بالاتي:

1) بنطاق ضرورة التحقيق، حيث أجازت المادة (80) إ.ج، ج لقاضي التحقيق أن يقوم بكافة إجراءات التحقيق في نطاق اختصاص المحاكم المجاورة لنطاق اختصاصه وفق شروط(2) هي :
   - أن تكون هناك ضرورة للانتقال خارج نطاق اختصاصه المكاني.
   - أن يخطر وكيل الجمهورية الذي يعمل في نفس دائرة اختصاصه.
   - أخطار وكيل الجمهورية في نطاق الاختصاص الذي تم التمديد إليه.

---

(1) الفقرة (4) من المادة (47) من ق. إ. ج. ج رقم (06 - 22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية..والجرائم المشار إليها في الفقرة الثالثة من نفس المادة والتي بموجبها يتم تمديد اختصاص قاضي التحقيق على كامل الترب الوطني هي جرائم المخدرات، وجرائم الإرهاب وتبييض الأموال، والجرائم المنظمة عبر الحدود الوطنية، وجرائم المساس بأنظمة المعالجة الآلية لمعطيات، والجرائم المتعلقة بالتشريع الخاص بالصرف.

(2) راجع: عبد الله أوهايبية، مرجع سابق، ص332.

- تحديد الأسباب التي جعلته يمدد دائرة اختصاصه المكانية في محضر المعاينة

2) كما يتم تمديد الاختصاص وفقا لحالات أخرى تتضمن جرائم معينة تشكل خطورة كبيرة على امن المجتمع، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم الإرهاب وتبييض الأموال، وجرائم المخدرات، بحيث يمكن لوكيل الجمهورية تمديد اختصاصه المحلي إلى دائرة اختصاص محاكم أخرى، كما أن قاضي التحقيق يستطيع القيام بأي إجراء معاينة أو تفتيش أو حجز على امتداد التراب الوطني، وكذلك يجوز تمديد اختصاص المحكمة إلى نطاق اختصاص محاكم أخرى.

كما أن المشرع الجزائري لم يقتصر على تمديد الاختصاص القضائي بمفهومة المادي التقليدي، بل إنه قد أجاز تمديد الاختصاص والقيام ببعض الإجراءات عن بعد في حال أن يتطلب الأمر تفتيش المنظومة المعلوماتية عن بعد، وكذلك حجز المعطيات، حيث ورد النص بأنه (.... إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك)[1].

وتظل مشكلة الاختصاص القضائي الوطني على مستوى الإقليم الوطني للدولة بالنسبة لجرائم المعلوماتية قائمة بالنسبة للتشريع اليمني، حيث لم يرد نص قانوني يتضمن تمديد الاختصاص القضائي إلى كافة الإقليم في حالة أن يتطلب الأمر ذلك، ولذلك فإن على المشرع اليمني تضمين نصوصه ما يوسع من امتداد الاختصاص القضائي لكافة الإقليم الوطني بالنسبة للإجراءات المتخذة بخصوص جرائم المعلوماتية أسوة بالتشريع الجزائري، وذلك أثناء قيامة بوضع نصوص قانونية لمواجهة جرائم المعلوماتية موضوعيا وإجرائيا.

ومع ذلك فيمكن إعمال نص المادة (117) التي تضمنت حق عضو النيابة العامة في ندب مأمور الضبط للقيام بإجراء أو أكثر من إجراءات التحقيق، حيث تضمنت في فقرتها الثانية بأن (لعضو النيابة العامة إذا دعاه الحال اتخاذ إجراء من الإجراءات خارج

(1) الفقرة الثانية من المادة (5) من القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

دائرة اختصاصه أن يكلف به عضو النيابة العامة المختص)[1].

فهذا النص وإن كان لا يسمح لعضو النيابة العامة باتخاذ أي أجراء خارج نطاق اختصاصه، إلا انه من ناحية أخرى يتيح له تكليف عضو النيابة المختص القيام بذلك الإجراء، وبالتالي يتحقق الهدف المتمثل بالقيام بذالك الإجراء وعدم إهماله وصولا لكشف الحقيقة، ومع ذلك فإن هذا الإجراء يقتصر على الانتقال المادي لا الافتراضي.

2- الاختصاص القضائي الدولي

تثار مشكلة الاختصاص القضائي الدولي بالنسبة للجرائم المرتكبة في نطاق المعلوماتية بصورة أكبر مما هي عليه على مستوى إقليم الدولة الواحدة، حيث يكون بإمكان الدولة وضع حد للمشكلة على المستوى الوطني أو المحلي، من خلال النصوص القانونية التي يمكن إقرارها بهذا البلد أو ذاك، لأن الجريمة محصورة في النطاق الإقليمي للدولة، ومعالجتها يرتبط بكل دولة على انفراد، بخلاف مشكلة الاختصاص القضائي على المستوى الدولي، لأن الجريمة في الأخيرة لا ترتبط بحدود إقليمية لدولة ما، بل على العكس من ذلك، فهي جريمة عابرة للحدود، بالإضافة إلى اختلاف التشريعات والنظم القانونية من دولة إلى أخرى في مواجهة تلك الجرائم، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، وفي هذه الحالة تخضع الجريمة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية[2]وسييتم إيضاح ذلك تباعا.

---

(1) راجع الفقرة (2) من المادة (117) إ. ج. ي رقم (13) لسنة 1994(ج.ر. ع.4/19 لسنة 1994.

(2) راجع:جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص 73.
وراجع:
Boudoumi Abderrahmane: Internet et droit pénal, intervention colloque <<l'espace électronique et le droit >> 9 et 11Mars2008, p.6.
.

أ- الاختصاص القائم على أساس مبدأ الإقليمية

وفقا لهذا المبدأ فإن المحاكم الجزائية في الدولة هي المختصة بنظر الجرائم التي تقع كلها، أو جزء منها على إقليمها، أيا كان شخص المتهم، أو صفته، وبغض النظر عن جنسيته [1].

وهذا المبدأ- الإقليمية- يرد عليه بعض الاستثناءات منها: عدم تطبيقه على رؤساء الدول ورجال السلك الدبلوماسي، إضافة إلى الاعتراف ببعض الأحكام الأجنبية بموجب نص قانوني أو معاهدة دولية [2].

وقد نص القانون اليمني على مبدأ الإقليمية من خلال نص المادة (3) من ق. ع حيث نصت على أن: (يسري هذا القانون على كافة الجرائم التي تقع على إقليم الدولة، أيا كانت جنسية مرتكبها، وتعد الجريمة مقترفة في إقليم الدولة إذا وقع فيه عمل من الأعمال المكونة لها، ومتى وقعت الجريمة كلها أو بعضها في إقليم الدولة يسري هذا القانون على من ساهم فيها ولو وقعت مساهمته في الخارج).

كذلك نصت المادة(236) في الفقرة الثانية منها على أنه :(أما إذا ارتكبت الجريمة جزئيا خارج الجمهورية وجزئيا داخلها، اختصت محليا المحكمة الواقع في دائرتها مكان ارتكاب أفعال الجريمة داخل الجمهورية) [3].

كما نص على ذات المبدأ القانون الجزائري من خلال نص المادة (3) من ق.ع والتي نصت على أن:(يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية) [4]، وهذا النص مأخوذ من القانون الفرنسي، حيث تضمن نص المادة (113- 2) تطبيق القانون الفرنسي إذا ارتكبت الجريمة أو احد عناصرها على الإقليم الفرنسي [5].

---

(1)عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها(المراقبة الدولية للسياسة الجنائية) ملخص الترجمة العربية لمرشد الأمم المتحدة1999، مرجع سابق، ص128

(2)حسني الجندي، مرجع سابق، ص55.

(3) أنظر المادة (3)، والفقرة(2) من المادة (236) من قانون العقوبات اليمني رقم (12)لسنة **1994** (ج.ر. ع 3/19،لسنة 1994).

(4) الفقرة (1) من المادة (3) من الأمر رقم (66- 156) المؤرخ في 8يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم.

(5)**Article 113-2**

(La loi pénale française est applicable aux infractions commises sur le territoire de la République.

L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire). =

كما يتم تطبيق الاختصاص القائم على مبدأ الإقليمية في اغلب الدول[1].

ومن خلال النصوص السابقة يتضح بأن القانون اليمني وكذالك الجزائري قد اشترطا لتطبيق مبدأ الإقليمية أن تكون الجريمة، أو أحد الأفعال المكونة لها قد تم ارتكابها في نطاق الإقليم الوطني للدولة[2]، حيث يكفي لانعقاد الاختصاص للمحاكم اليمنية والجزائرية أن ترتكب الجريمة بكامل أركانها في اليمن أو الجزائر، أو أي فعل من الأفعال المكونة لها سواء أكانت الجريمة بسيطة، أم مركبة، مستمرة، أم متابعة، أم من جرائم الاعتياد.

ولا يهم بعد ذلك مكان وجود الجاني، فالمعيار في هذه الفرضية هي بمكان ارتكاب الجريمة كلها، أو بعضها كمن حاز شيا مسروقا وتنقل به في عدة دول فإن جريمة الإخفاء تكون متحققة في كل الدول، فاعلا أو شريكا.

ومع إمكانية تطبيق هذا المبدأ - الإقليمية - على جرائم المعلوماتية وعلى وجه الخصوص المرتكبة منها عن طريق الإنترنت، إلا أن ذلك قد يثير بعض المشكلات منها مشكلة تنازع الاختصاص القضائي لأكثر من دولة، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي

= ووفقا لمبدأ الإقليمية وفقا للنص الفرنسي سالف الذكر فإن القانون الفرنسي يطبق على كثير من الجرائم التي ترتكب بواسطة الانترنت بمجرد وقوع احد العناصر المكونة للجريمة، أو حتى وقوع النتيجة على الإقليم الفرنسي، فيطبق القانون على الرسالة ذات الطابع الإجرامي، أو الصورة الإباحية، أو العبارات التي تحض على الكراهية العنصرية والتي تنتشر عبر شبكة الانترنت، بصرف النظر عن الدولة التي صدرت منها هذه الرسالة، طالما أنه يمكن الدخول إليها من فرنسا، لان تلقي المستخدم في إقليم الدولة لهذه الرسالة، أو تلك الصورة يعد أحد العناصر المكونة للجريمة طبقا للمادة (113-2)ع.ف جديد، بغض النظر عن أن يكون الفعل معاقبا عليه أم لا في بلد المنشأ، كما يعد فعل التوصيل بالمعلومات غير المشروعة احد العناصر المكونة للجريمة، فمجرد التوصيل بموقع يقوم بتقليد المصنفات يكفي لتحقيق ماديات الجريمة حيث أن فعل الإذاعة أو البث يتحقق في نقطة التوصيل التي تتم عن طريق متعهد التوصيل، والتي تمكن أي مستخدم من الدخول على أي المعلومات الموجودة على أي موقع، ويترتب على ذلك بأن تحديد مكان الحاسب الخادم الخاص بالإيواء في الخارج لا ثر له على ارتكاب الجريمة على الإقليم الوطني، طالما يمكن الاطلاع على المعلومات في الإقليم الوطني فإن الاختصاص ينعقد لقضاء هذا الإقليم، وكذلك ينعقد الاختصاص بالنسبة لجريمة تقليد المصنفات لان نقطة التوصيل بتلك المواقع قد تمت على هذا الإقليم، كما ينعقد الاختصاص في حالة أن تم النسخ على الإقليم. ومن التطبيقات القضائية في فرنسا لمبدأ إقليمية النص الجنائي، محاكمة رئيس شركة فرانس نت (France net) وورلد نت (World net) لأنهما قاما بنشر صور دعارة أطفال متأتية من الخارج وذلك بالمخالفة للمادة (227- 23)من القانون الفرنسي . راجع: جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص47، وص50.

([1]) في بريطانيا يشترط لاختصاص القضاء البريطاني أن تكون الواقعة الإجرامية لها ارتباط ببريطانيا يستوي في ذلك أن يكون مرتكب الواقعة قد ارتكبها في بريطانيا، أو كانت نتيجتها قد امتدت إلى بريطانيا، بصرف النظر عن مكان إقامة الفاعل، فيكفى بأن يكون نشاط الفاعل قد تضمن تعديلات على حاسوب في بريطانيا، بينما يختص القضاء الأمريكي بنظر كل واقعة يتحقق فيها أي فعل في أمريكا، كذلك فقد عمل بمبدأ النتيجة الإجرامية.راجع: عمر محمد ابو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص910، وص911.

([2]) راجع المادة (3) من ق.ع.ي، والمادة (586) من ق. إ. ج.ج.

هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.

فشبكة الإنترنت ليس لها مقر في دولة معينة، ولا تخص شخصا أو جهة معينة، وتوجد موزعة على الكرة الأرضية[1]، وهي عبارة عن تجمع عدد كبير من الشبكات مختلفة النوع والمصدر والوظيفة، وترتبط بها الخطوط الهاتفية من كل دول العالم، والأشخاص من كل دول العالم يستطيعون تبادل الأفكار والمعلومات بكل حرية، وهي بذلك تمثل الجهات والأفراد الذين يستخدمونها في تبادل المعلومات بكل حرية، ولذلك فهي لا تخضع لرقابة وسيطرة دولة معينة، ويترتب على ذلك عدم وجود قانون جنائي يحكمها، بل على العكس تتعدد القوانين الجنائية التي تطبق عليها بتعدد الدول التي ترتبط بها، باعتبار أن القانون الجنائي يتعلق بسيادة الدولة، وهنا تكمن المشكلة [2].

كما أن عدم فاعلية المحاكمة عن الجرائم المعلوماتية التي تقع في الخارج، تعد إحدى مشكلات الاختصاص القضائي، نظرا لتدويل الجرائم المرتكبة عن طريق الإنترنت، مما يجعل منعها والعقاب عليها امرأ احتماليا في ظل الوضع الراهن للأنظمة

([1]) تنقسم الشبكات إلى نوعين: الشبكات المحلية (LAN) (LOCAL AREA NETWORKS) تستخدم داخل منطقة معينة أو حيز معين، والشبكات علي نطاق واسع (WAN)(WIDE AREA NETWORKS) تربط بين عدة شبكات محلية معا في إطار واحد باستخدام التلفون أو القمر الصناعي أو الميكروويف، ويعد الإنترنت جزء من ثورة الاتصالات، وتعرف بشبكة الشبكات، وكانت البداية في 2 -1- 1969-عندما شكلت وزارة الدفاع الأمريكية فريقا من العلماء للقيام بمشروع بحثي عن تشبيك الحاسبات،وركّزت التجارب علي تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة، ومن ثم نقل هذه الأجزاء بشكل وطرق مستقلة حتى تصل مجتمعة إلى هدفها، وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب، ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة، فإن الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها عن أي طريق آخر بديل إلى خط النهاية، وكان ذلك ردا على قمر صناعي تجسسي سمي سبوتنيك(sputnik) أطلقته روسيا وكانت تستطيع من خلاله تحديد الأهداف بدقه، ومن ثم أمكانية القيام بضربها وعلى رأسها وسائل الاتصالات لجعل الأمريكيين يفقدون السيطرة، و تطور المشروع وتحول إلى الاستعمال السلمي حيث انقسم عام 1983 إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) ، كما احتفظت بغرضها الأساسي وهو خدمة الاستخدامات العسكرية ، وسميت الشبكة الثانية باسم (MILNET) للاستخدامات المدنية أي تبادل المعلومات وتوصيل البريد الإلكتروني ومن ثم ظهر مصطلح " الإنترنت " حيث أمكن تبادل المعلومات بين هاتين الشبكتين، وفي عام 1986 أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وسميت (NSFNET) والتي أصبحت العمود الفقري وحجر الأساس لنمو وازدهار الإنترنت في أمريكا، ومن ثم دول العالم الأخرى، وقد تم تطوير شبكة أخرى للانترنت في 2002 ، وتتميز بالسرعة في نقل وتبادل المعلومات، وهي شبكة انترنت 2، حيث تم إنشاء هذه الشبكة في الولايات المتحدة لتخدم البحث العلمي، وتم وصل الجامعات ومراكز الأبحاث بهذه الشبكة، ويرتبط بها 130 جامعة ومركز علمي، ومركزها الرئيسي في شيكاغو، ولهذه الشبكة ميزات كثيرة منه سرعة إرسال البيانات، والإرسال لعدة مواقع في نفس الوقت، وجودة الصور المرسلة. راجع: محمد عبد الله المنشاوي، الانترنت بدايته وتعريفه واهم جرائمه، أكاديمية نايف للعلوم الأمنية، المملكة العربية ألسعوديه، ت.د 30/ 6/ 2010على الرابط:

law.htm20%the20%http://www.minshawi.com/old/internetcrim-in

وراجع، محمد أمين الرومي، مرجع سابق، ص122 وما بعدها.

وفي الإنترنت 2 راجع: مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، مرجع سابق، ص229.

([2]) راجع جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص42.

القانونية، فيكون من السهل على خدمة صدر حكم قضائي بمنعها أن تغير اسمها وتعود لبث المعلومات غير المشروعة من مكان آخر، وهذه العملية يمكن أن تتم في وقت أقصر من الوقت اللازم لاتخاذ الإجراءات القضائية المستعجلة[1].

ومن الإشكاليات أيضا في تطبيق القانون الوطني على الجرائم التي تقع كلها أو جزء منها في إقليم الدولة، ازدواجية الاختصاص حيث يختص بها القانون الأجنبي في نفس الوقت الذي تدخل في اختصاص القانون الوطني، وذلك قد يؤدي إلى الإطاحة بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة، حيث إن امتداد الاختصاص لقضاء الدولة التي تم تلقي الرسالة غير المشروعة فيها، وقضاء الدولة التي تم البث منها يؤدي إلى محاكمة الجاني أكثر من مرة.

كما أن من المشكلات التي تعيق تطبيق الاختصاص القضائي القائم على مبدأ الإقليمية في مجال الجرائم المعلوماتية، تتمثل في حالة أن يكون مزود الانترنت تابع لمزود أخر موجود في دولة أخرى، أو يكون مزود الإنترنت الأساسي موجود في دولة بينما المزودات الفرعية في أكثر من دولة، فأي من قضاء تلك الدول يكون مختصا، وأي من القوانين يكون واجب التطبيق[2].

ومع أن بعض القوانين تعالج مسألة الاختصاص القضائي وفقا لمبدأ إقليمية النص بصورة مغايرة لما هو معمول به في أغلب التشريعات، حيث يرتبط تطبيق النص الإقليمي على الجريمة بشرط أن تكون مجرمة أيضا في البلد الآخر، وأن تكون ثابتة بموجب حكم قضائي في البلد الأجنبي، ومن تلك القوانين قانون العقوبات الفرنسي من خلال نص المادة (113-5) حيث تضمنت تطبيق قانون العقوبات الفرنسي على كل من ارتكب فعل في إقليم الجمهورية يجعله شريكا في جناية، أو جنحة وقعت في الخارج، إذا

([1]) جميل عبد الباقي الصغير، نفس المرجع، ص58.

([2]) أتجه القضاء الألماني إزاء الاختصاص القضائي في حالة أن يكون مزود الإنترنت الأساسي خارج المانيا والمزود الفرعي في ألمانيا إلى اعتبار القضاء الألماني مختصا، إزاء المسؤولية الجنائية لمزود الإنترنت الفرعي، طالما والبث يصل إلى ألمانيا، ففي قضية شركة (CompuServe 1998) – وجود مواقع دعارة- قضت محكمة ميونخ في حكمها الصادر في 1998/5/28 بمسؤولية الشركة، والتي تعد فرع للشركة الأم في الولايات المتحدة الأمريكية، وأقرت المحكمة مسؤولية المزود الفرع باعتباره مزود استضافة لعلاقته الوطيدة بالمركز الرئيس في الولايات المتحدة الأمريكية، حيث أن المركز الرئيسي يعد طرق بث إلى الخوادم الأخرى التابعة له عبر العالم. وكذلك فقد أقر القضاء الفرنسي ذات المبدأ في قضية اتحاد الطلبة اليهود ضد Yahoo ، حيث اتجه القضاء الفرنسي إلى التقرير باختصاصه في هذه الدعوى حتى لو كانت Yahoo فرنسا فرعا لمركز رئيسي في الولايات المتحدة طالما أن البث يصل إلى فرنسا. راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص916، ص917.

كانت الجناية أو الجنحة معاقبا عليهما في القانون الفرنسي والقانون الأجنبي، وثابتة بموجب حكم قضائي من البلد الأجنبي [1].

والمشكلة في هذه الحالة تتمثل في صعوبة تحديد مكان ارتكاب الجريمة الأصلية، لكون تجريم الفعل الأصلي في الخارج هو شرط أولي لعقد الاختصاص القضائي للقضاء الفرنسي، وبالتالي فإن عدم معرفة الدولة التي تبث منها المعلومات المجرمة يحول دون محاكمة الشريك في فرنسا، يضاف إلى ذلك تعقد شبكة الإنترنت، وتنوع طرق استخدامها، بحيث لا يسمح بتحديد مكان ارتكاب الجريمة، ذلك أنه إذا كان من السهل تحديد مكان ارتكاب الجريمة عندما تكون المعلومات غير المشروعة مرسلة في رسالة الكترونية، حيث يمكن تحديد محل إقامة كل من المرسل والمرسل إليه، فإن الأمر يكون صعبا عندما توجد المعلومات غير المشروعة على صفحة الويب (Page web)، حيث إنه وأن أمكن تحديد مكانها في بلد المتعهد الذي يقوم بإيوائها، إلا أنه يمكن رؤيتها في العالم أجمع، وذلك ينطبق عل قوائم المناقشات، أو المؤتمرات التي لا تتمركز في مكان محدد، كما أن المعلومات غير المشروعة والمرسلة عبر مزودي الويب (Server web) تكون البلد الأصلي لها غير معروفة [2].

وبالتالي وإزاء المشكلات المتعلقة بالاختصاص القضائي القائم على مبدأ الإقليمية في جرائم المعلوماتية فلابد من وجود تعاون دولي لتخطي مثل هذه المشكلات، من خلال المعاهدات الثنائية، أو الدولية بهذا الشأن تجعل قضاء الدولة التي شرعت في اتخاذ الإجراءات، أو الدولة الأكثر تضررا من الجريمة المعلوماتية هي المختصة وعلى باقي الدول التي تحققت فيها الجريمة أو جزء منها التعاون مع قضاء تلك الدولة وصولا لمعاقبة الجاني.

([1]) **Article 113-5**
La loi pénale française est applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi française et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère.
http://www.legislationline.org/documents/section/criminal-codes

([2]) راجع: جميل عبد الباقي الصغير، الجوانب الإجرائية في جرائم الإنترنت، مرجع سابق، ص52.

إضافة إلى تفعيل التعاون ألامني بين مختلف المؤسسات الأمنية فيما بينها، وعن طريق الانتربول الدولي، بهدف تمكن الأجهزة الأمنية من الحصول على البيانات والمعلومات المتعلقة بتلك الجرائم، وتحديد مكان المجرم في الوقت المطلوب [1].

ب- الاختصاص القائم على أساس مبدأ الشخصية

يقوم الاختصاص القضائي وفقا لهذا المبدأ على اختصاص القضاء في الدولة التي يحمل الجاني جنسيتها في حال ارتكابه جريمة في الخارج، وذلك ما يسمى بالاختصاص الشخصي الإيجابي.

وقد وسعت بعض الدول من الاختصاص القائم على مبدأ الشخصية، حيث لم تقتصر على جنسية الجاني، بل إنها أضافت جنسية المجني عليه كمعيار لتطبيق قضائها على الجريمة التي ترتكب ضد أحد مواطنيها في الخارج وذلك ما يسمى بالاختصاص الشخصي السلبي، ووفقا لذلك يمكن تطبيق قانون الدولة على مواقع الدعارة في الخارج التي ينشئها من يحمل جنسيتها، بشرط أن يكون هذا الفعل معاقبا عليه في الدولة الأخرى[2] .

(1) ومثال للتعاون الدولي في مجال تحديد مكان مرتكب الجريمة تمكن مكتب التحقيقات الفدرالي الأمريكي بالتعاون مع شرطة ويلز في بريطانيا من تحديد مكان رافائيل جري 18 عام ، بريطاني الجنسية والذي قام بكشف تفاصيل بطاقات الائتمان الخاصة ببيل جيتس (صاحب شركة مايكروسوفت وأغنى رجل بالعالم) و26 الف آخر من مختلف أنحاء العالم، حيث تسبب في خسائر بلغت 3 ملايين دولار. راجع مصطفى محمد موسى ، أساليب إجرامية بالتقنية الرقمية، مرجع سابق، ص63.

(2) تقر بعض الدول ومنها فرنسا الاختصاص القضائي بموجب مبدأ الاختصاص الشخصي بجانبيه السلبي والإيجابي، والجانب السلبي يعني خضوع مرتكب الجريمة التي يكون المجني عليه فيها فرنسيا للقضاء الفرنسي، فمسألة الاختصاص تتعلق بجنسية المجني عليه، ومبدأ شخصية النص الجنائي في جانبه السلبي لا تقره أغلب القوانين. أما الجانب الايجابي للاختصاص الشخصي فيتعلق بالجاني وليس بالمجني عليه، حيث يشترط أن يكون الجاني فرنسيا، وهذا المبدأ مقر من أغلب القوانين. راجع: محمد أبو العلاء عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد، دار الفكر العربي ، القاهرة، 1997،ص31، شريف سيد كامل، تعليق على قانون العقوبات الفرنسي الجديد، ط1، دار النهضة العربية، القاهرة، 1998، ص80، و راجع نصوص المواد (113-6 و113-7)من قانون العقوبات الفرنسي الجديد 2004.حيث ورد النصان بالفرنسي على النحو التالي:

Article 113-6

La loi pénale française est applicable à tout crime commis par un Français hors du territoire de la République.

Elle est applicable aux délits commis par des Français hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis.=

=Il est fait application du présent article lors même que le prévenu aurait acquis la nationalité française postérieurement au fait qui lui est imputé.

Article 113-7

La loi pénale française est applicable à tout crime, ainsi qu'à tout délit puni d'emprisonnement, commis par un Français ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment de l'infraction.

http://www.legislationonline.org/documents/section/criminal-codes

وقد نص القانون اليمني على مبدأ الشخصية من خلال المادة(246) والتي نصت على (تختص المحاكم اليمنية بمحاكمة كل يمني ارتكب خارج إقليم الدولة فعلا يعد بمقتضى القانون جريمة، إذا عاد إلى الجمهورية، وكان الفعل معاقبا عليه بمقتضى قانون الدولة الذي ارتكبت فيه)[1].

كما نصت المادة (582)من القانون الجزائري على أن (كل واقعة موصوفة بأنها جناية معاقب عليها من القانون الجزائري، ارتكبها جزائري في خارج إقليم الجمهورية يجوز أن تتابع ويحكم فيها في الجزائر.

غير أنه لا يجوز أن تجرى المتابعة أو المحاكمة إلا إذا عاد الجاني إلى الجزائر، ولم يثبت أنه حكم عليه نهائيا في الخارج، وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة، أو سقطت عنه بالتقادم، أو حصل العفو عنها).

كما نصت المادة (583) على: (كل واقعة موصوفة بأنها جنحة سواء في نظر القانون الجزائري أم في تشريع القطر الذي ارتكبت فيه، يجوز المتابعة من أجلها والحكم فيها إذا كان مرتكبها جزائريا.

ولا يجوز أن تجري المحاكمة أو يصدر الحكم إلا بالشروط المنصوص عليها في الفقرة الثانية من المادة (582)، وعلاوة على ذلك فلا يجوز أن تجري المتابعة في حالة ما إذا كانت الجنحة مرتكبة ضد أحد الأفراد إلا بناء على طلب النيابة العامة بعد إخطارها من الشخص المضرور، أو ببلاغ من سلطات القطر الذي ارتكبت فيه الجريمة) [2].

وطبقا للنصوص السابقة فإنه يطبق النص الجزائي اليمني على كل من يحمل الجنسية اليمنية، وكذلك الجزائري على كل من يحمل الجنسية الجزائرية إذا توافرت عدد من الشروط منها:

- أن يكون الفعل المجرم في القانون اليمني والجزائري مجرم في قانون البلد الذي اقترف فيه.

([1]) المادة (246) من قانون الإجراءات الجزائية اليمني .
(2) المادة (582)، والفقرة (2) من المادة (583) من الأمر الجزائري رقم (66-155) المؤرخ في 8 يونيو 1966بشأن الإجراءات الجزائية المعدل والمتمم.

- أن يشكل الفعل الذي تم اقترافه في الخارج جريمة جسيمة أو غير جسيمة في القانون اليمني، وجناية أو جنحة في القانون الجزائري[1].
- أن يعود المتهم إلى اليمن إذا كان يمني، وإلى الجزائر إذا كان جزائري.
- أن لا يكون وفقا للقانون الجزائري قد حكم عليه بحكم نهائي في الخارج، وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة، أو سقطت عنه بالتقادم، أو حصل العفو عنها، بينما لم يتضمن القانون اليمني مثل هذا الشرط، وبالتالي فإنه وفقا للقانون اليمني يمكن معاقبة اليمني على جريمته التي ارتكبت في الخارج مرتين بخلاف القانون الجزائري .
- يشترط في القانون الجزائري أن يكون الفاعل يحمل الجنسية الجزائرية وقت ارتكاب الفعل، بينما يكتفي القانون اليمني باكتساب الجنسية حتى بعد اقتراف الفعل [2].
- يجب أن يكون النظر في الجريمة المرتكبة من قبل المحكمة المختصة بموجب طلب من النيابة العامة بعد إخطارها من الشخص المضرور، أو ببلاغ من سلطات القطر الذي ارتكبت فيه الجريمة.
- والقانون اليمني وكذلك القانون الجزائري لا يعرفان الوجه السلبي للاختصاص القائم على مبدأ الشخصية، فجنسية المجني عليه في كلا القانونيين ليست شرطا لتطبيق قضائهما على الجريمة المرتكبة في الخارج ضد من يحمل جنسيتيهما، باستثناء أن تكون الجريمة المرتكبة جناية كانت أو جنحة قد ارتكبت على متن طائرات أجنبية وكان المجني عليه جزائري إذا هبطت في الجزائر، أو تم القبض على الجاني فيها، وقد تضمن هذا الاستثناء القانون اليمني [3].

والاختصاص القضائي وفقا لمبدأ الشخصية في مجال الجريمة بشكل عام والجريمة المعلوماتية بشكل خاص يثير العديد من المشكلات منها:

(1) تنقسم الجرائم وفقا لقانون العقوبات اليمني إلى جرائم جسيمة وجرائم غير جسيمة، والجرائم الجسيمة هي: ما عوقب عليه بحد مطلق، أو بالقصاص بالنفس، أو بإبانة طرف أو أطراف، وكذلك كل جريمة يعزر عليها بالإعدام، أو بالحبس مدة تزيد على ثلاث سنوات، أما الجرائم غير الجسيمة فهي: التي يعاقب عليها بالدية، أو بالإرش، أو بالحبس مده لا تزيد على ثلاث سنوات، أو الغرامة. بينما تنقسم وفقا لقانون العقوبات الجزائري إلى جنايات وجنح ومخالفات، والجنايات هي: ما عوقب عليها بالإعدام، أو السجن المؤبد، أو السجن المؤقت بين خمس سنوات وخمسة وعشرين سنة، أما الجنح في القانون الجزائري فهي: ما عوقب عليها بالحبس من شهرين إلى خمس سنوات باستثناء الحالات التي ينص عليها القانون، والغرامة التي لاتتجاوز20.000 دج. راجع: المادة(16) والمادة (17) من ق. ع.ي، والمادة(5) والمادة (27)من ق. ع. ج.

(2) راجع: المادة (248) إ.ج.ي.

(3) راجع: الفقرتين الثانية والثالثة من المادة (590) إ.ج.ج، وكذلك المادة (254) إ.ج.ي.

- عدم اختصاص قضاء الدولة في الجريمة المرتكبة في الخارج ممن يحمل جنسيتها، إذا لم تعتبر جريمة في الدولة المرتكبة فيها، فالاختصاص لا ينعقد بالنسبة للمعلومات، والصور التي تبث من الخارج، إذا كانت غير مجرمة في بلد المنشأ حيث تم البث، مع أنها جريمة في الدول التي يصلها البث، وفي مثل هذه المسألة - حينما لا يكون القانون الوطني مختصاً في نظر الواقعة - تثار المشكلة بالنسبة لمن أصابه الضرر من الجريمة المرتكبة، حيث يجب عليه أن ينتقل إلى الدولة التي ارتكبت منها الجريمة لرفع دعواه، وتثار المشكلة بصورة أكبر كون الفعل غير معاقب عليه في هذه الدولة[1].
- أن العقاب على فعل وقع في الخارج يكون غير فعال، لأن تنفيذ العقوبات سيصطدم بعقبات جمة، في ظل العدد القليل من الدول التي وقعت على اتفاقية تسليم المجرمين، مقارنة بعدد الدول المرتبطة بالإنترنت، ولذلك فإن الرأي المطروح هو إيجاد قانون دولي جنائي على غرار القانون الدولي الخاص ليطبق على الجرائم التي ترتكب على الإنترنت أو بواسطتها[2].

ج- الاختصاص القائم على أساس مبدأ العينية

وفقا لهذا المبدأ فإن التشريع الجنائي الوطني يمتد ليطبق على الجرائم التي ترتكب في الخارج بغض النظر عن جنسية مرتكبها، وينبع هذا المبدأ من ما للدولة من حق في الدفاع الذاتي عن كافة صور الاعتداء على مصالحها الأمنية والمالية، ولو وقعت الجريمة خارج إقليمها[3]، حيث يقوم الاختصاص القضائي وفقا لهذا المبدأ على اختصاص قضاء الدولة في نظر نوع معين من الجرائم، هي الجرائم التي تمس أمنها ومصالحها، بغض النظر عن أن يكون مرتكب الجريمة يحمل جنسيتها أو لا، وبغض النظر عن أن يكون مقترف الجريمة متواجداً في إقليمها أو خارجه [4].

---

(1) أحمد عبد الكريم سلامة، الإنترنت والقانون الدولي الخاص، مرجع سابق، ص38. وراجع فهد سلطان محمد أحمد بن سليمان، مرجع سابق، ص97.

(2) جميل عبد الباقي الصغير، الجوانب الإجرائية في جرائم الإنترنت، مرجع سابق، ص51.

(3)انظر المادة(247) والمادة (248)من قانون العقوبات اليمني رقم(12) لسنة 1994 واللتان تضمنتا النص على اختصاص القضاء اليمني بنظر الجرائم التي تمس أمن الدولة الداخلي أو الخارجي وفقا للمواد(121 وما بعدها من ذات القانون)، وكذلك المادة(588) أ.ج.ج .

(4) تقر أغلب التشريعات مبدأ الاختصاص القضائي العيني، بحيث تتيح لقضائها الفصل في أي قضية تتعلق بمصالحها وأمنها القومي، ومن تلك التشريعات قانون العقوبات الفرنسي من خلال نص المادة(113- 10) حيث يطبق القانون الفرنسي على الجنايات والجنح التي ترتكب في الخارج وتشكل اعتداء على المصالح الأساسية=

وقد نص القانون اليمني على هذا المبدأ من خلال نص المادة (247) حيث نصت على أن: (تختص المحاكم اليمنية بمحاكمة كل من ارتكب خارج إقليم الدولة جريمة مخلة بأمن الدولة مما نص عليه في الباب الأول من الكتاب الثاني من قانون العقوبات[1] أو جريمة تقليد أو تزييف أختام الدولة أو إحدى الهيئات العامة أو تزوير عمله وطنية متداولة قانونا أو إخراجها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها)[2].

كما نص على مبدأ العينية القانون الجزائري من خلال نص المادة (566) حيث نصت على : (كل أجنبي ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية، أو تزييفا للنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر، تجوز متابعته ومحاكمته وفقا للقانون الجزائري إذا القي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها) [3].

ولم يقتصر المشرع الجزائري على هذا النص الذي كان يعالج مسألة الاختصاص القضائي وفقا لمبدأ العينية بالنسبة للجرائم التقليدية، بل أنه ومن خلال القانون الجديد الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي

=للأمة المنصوص عليها في الباب الأول من الكتاب الرابع من قانون العقوبات وكذلك تقليد وتزوير أختام الدولة وتزييف العملة المعدنية والورقية أو السندات العامة والمعاقب عليها بالمواد 422-1 ،444 -1، وعلى أية جناية أو جنحة ترتكب ضد أعضاء وأماكن البعثات الدبلوماسية والقنصلية الفرنسية بالخارج .والنص بالفرنسي :

Article 113-10

(Loi nº 2001-1168 du 11 décembre 2001 art. 17 Journal Officiel du 12 décembre 2001)

La loi pénale française s'applique aux crimes et délits qualifiés d'atteintes aux intérêts fondamentaux de la nation et réprimés par le titre Ier du livre IV, à la falsification et à la contrefaçon du sceau de l'Etat, de pièces de monnaie, de billets de banque ou d'effets publics réprimées par les articles 442-1, 442-2, 442-5, 442-15, 443-1 et 444-1 et à tout crime ou délit contre les agents ou les locaux diplomatiques ou consulaires français, commis hors du territoire de la République.

وكذلك قانون العلاقات الخارجية الأمريكي حيث يجعل الاختصاص القضائي الأمريكي قائما، طالما كان هناك سلوكا ذا تأثير على الإقليم الأمريكي، كذلك ينعقد الاختصاص للقضاء الأمريكي إذا كان هناك مساس بالأمن القومي الأمريكي، حتى لو ارتكب السلوك بكامله خارج أمريكا. راجع: عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص906.

(1) تضمن قانون العقوبات اليمني في الباب الثاني منه الجرائم الماسة بالأمن القومي للدولة من خلال المواد (من 125 إلى 136) والتي منها المساس باستقلال الجمهورية أو وحدتها أو سلامة أراضيها، وأي فعل يهدف إلى إضعاف القوات المسلحة، أو التخابر لدى دولة أجنبية، وكذلك الجرائم الماسة بالأمن الداخلي للدولة، فهذه الجرائم وغيرها مما تضمنتها نصوص المواد المذكورة تخضع لنصوص القانون اليمني والقضاء اليمني بغض النظر عن جنسية مرتكبيها، وبغض النظر عن مكان ارتكابها.

(2) المادة (247) من ق.ع. ي.

(3) المادة (588) من الأمر رقم (66-155) المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

تضمن في إحدى مواده تمديد الاختصاص القضائي بالنسبة لهذه الجرائم حيث ورد النص كالتالي: (زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني)[1].

من خلال النصوص السابقة يتضح بأن المشرعين اليمني والجزائري قد تضمنا اختصاص القضاء الوطني في كلا البلدين في الجرائم الماسة بالأمن القومي للدولة، وكذلك جرائم تزييف النقود والأوراق المصرفية الوطنية لكلا البلدين إذا تم ارتكابها في الخارج من قبل أجنبيي، ومع أن النص في القانون اليمني يوحي بعدم اقتصار الفاعل على الأجنبي كما في النص الجزائري، بل يشمل اختصاص القضاء اليمني سواء أكان الجاني يمنيا أم أجنبيا في حالة ارتكابه إحدى الجرائم المشار إليها، إلا أن ذلك سيوجد خلط بين الاختصاص القائم على مبدأ الشخصية والاختصاص القائم على أساس مبدأ العينية، وبالتالي فالنص المشار إليه يقتصر على الأجنبي الذي يرتكب إحدى الجرائم المشار إليها وفقا لمبدأ العينية، وذلك لورود نص أخر يتعلق بالاختصاص القائم على مبدأ الشخصية وفقا لم تم إيضاحه.

وقد تميز المشرع الجزائري عن اليمني في النص على تمديد الاختصاص القضائي بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال عندما تستهدف تلك الجرائم مؤسسات الدولة الجزائرية، أو الدفاع الوطني، أو المصالح الإستراتيجية للاقتصاد الوطني، فتلك الجرائم يمكن أن ترتكب بواسطة الإنترنت، في حالة أن يكون الموقع الذي ارتكبت من خلاله الجريمة يقع خارج الدولة، ومن تلك الجرائم جريمة السعي أو التخابر لدى دولة أجنبية، وجريمة تسليم أو إفشاء أسرار الدفاع وغيرها من الجرائم الماسة بالأمن القومي للدولة[2]. كما يمكن أن ينطبق على جرائم تزييف النقود والأوراق المالية الوطنية بغض النظر عن الوسيلة التي استخدمت في التزوير تقليدية كانت أو الكترونية.

---

(1) المادة (15) من القانون رقم (09-04) المؤرخ في 2009/8/5 يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(2) المواد (من 121- 128) من ق.ع.ي، والمواد (61 إلى 83)من ق.ع.ج.

ويمتد الاختصاص في بعض الدول في قضايا الإنترنت إلى مكان تحقق النتيجة، فيختص قضاء الدولة التي تحققت فيها النتيجة [1].

وكما سبق القول بوجود مشكلات تتعلق بالاختصاص القضائي سواءٌ الإقليمي منها أم الشخصي، فكذلك الاختصاص العيني إذ تواجه تطبيقه العديد من المشكلات التي تعيق التنفيذ ومنها:

- مشكلة تعارض الاختصاص وفقا لمبدأ العينية مع الاختصاص وفقا لمبدأ الإقليمية في حالة أن تكون الجريمة المرتكبة وفقا لمبدأ العينية مجرمة في قانون الدولة الأخرى التي اقترفت فيها، فهنا تثار مسألة تنازع الاختصاص مابين الدولة المقترفة فيها الجريمة وفقا لمبدأ الإقليمية والدولة الأخرى التي تعد تلك الجريمة من الجرائم التي يناط بقضائها نظرها وفقا لمبدأ العينية، وبالتالي فقد يحاكم الشخص على فعله مرتين.
- لأن السلوك والنتيجة يمثلان شطري الجريمة في الجرائم المعلوماتية التي ترتكب عن طريق الشبكات، فإن كل محاكم مكان النشاط الإجرامي ومكان النتيجة تكون مختصة بنظر الجريمة [2]، وبناء على ذلك فإذا تم البث لفيروس معين ، وذلك ما يمثل السلوك الإجرامي، في مكان وتحققت النتيجة المتمثلة بتدمير المعلومات أو خلاف ذلك من النتائج المتعلقة بالتلاعب بالبيانات، أو تحويل أموال أو غير تلك من النتائج في مكان آخر، فإن الاختصاص سيتحقق للمحكمة الواقعة في مكان بث الفيروس وكذلك للمحكمة الواقعة في مكان تحقق النتيجة.
- ومن المشكلات التي تتعلق بالاختصاص القضائي هي أن اختصاص القضاء بنظر جرائم الكمبيوتر والقانون المتعين تطبيقه على الفعل لا يحظى دائما بالوضوح أو القبول أمام حقيقة أن غالبية الأفعال ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، وهو ما يبرز أهمية

(1) ومن تلك القضايا ما حدث في الولايات المتحدة الأمريكية عام 1991 من قيام شخص وزوجته بالسماح للغير بالدخول إلى نظام النشر الكمبيوتري الخاص بهم، الذي يحتوي على مواد فاضحة وداعرة لحوالي 14.000 صورة داعرة بملفات(GIF)، وكذلك مراسلات داعرة، وبعد محاولات فاشلة لإدانتهم بولاية (California) قام رجال المباحث بإنزال (Download) الملفات التي تحمل الصور والمراسلات الإباحية في ولاية (Tennessee) وتمت محاكمتهم، ومن ثم عقابهم وفقا لمبدأ اختصاص قضاء الولاية التي تحققت النتيجة بها (Tennessee) .ولم يفلحا في استئنافهما بالطعن في عدم الاختصاص. راجع عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص908.

(2) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص62، وص63.

امتحان قواعد الاختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة تطال هذه الجرائم أم أنه يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات تتعلق بالاختصاص القضائي.

- كما يرتبط بمشكلات الاختصاص وتطبيق القانون، مشكلات تتعلق بامتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود، وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية [1].

وخلاصة ما تم إيضاحه فإن مشكلة الاختصاص القضائي قد أضحت معقدة في ظل عدم وجود اتفاق دولي ينظم المسألة، وذلك في ظل ما تتمتع به شبكة المعلوماتية من فقدان السيطرة أو الرقابة عليها، وعلى المعلومات المتداولة عبرها، فمع أنه توجد عدد من الدول المتقدمة في مجال التكنولوجيا الرقمية تقوم بالرقابة الإلكترونية والتحليل الآلي لكل معلومة أو رسالة شاردة أو واردة منها أو إليها، إلا أن الكم الهائل من المعلومات قد تعيق ذلك إلا حد ما، وإذا كان ذلك العمل غير مرغوب به في مجال التجسس الإلكتروني بين الدول أو الأفراد، وفقا لما تم التنويه إليه سابقاً، فإن ذلك يؤكد لنا أنه في ظل عدم التعاون الدولي في متابعة وضبط الجرائم ذات الطابع الرقمي، فستظل مسألة الاختصاص القضائي تثير العديد من الإشكاليات،خاصةً في الجوانب الإجرائية المتعلقة بالتفتيش والضبط.

وبالتالي ففي جرائم المعلوماتية يحتاج الأمر إلى إعادة نظر، ولا مانع من تقرير نص يمكن بمقتضاه السماح لرجال الضبط القضائي بالانتقال عبر العالم الافتراضي للتعاون مع جهات ضبط دولية خارج نطاق اختصاصه المكاني[2].

([1]) يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل تم تقديمها إلى مؤتمر الأمن العربي، أبو ظبي ،10-2002/2/12.منشوره في الإنترنت،ت.د 2009/1/30 على الرابط:
http://doc.abhatoo.net.ma/IMG/doc/dro35.doc

([2])عمر محمد أبو بكر يونس،الجرائم الناشئة عن استخدام الإنترنت،مرجع سابق،ص823.

المطلب الثاني

الإثبات بالدليل المعلوماتي

ما زالت حجية الأدلة المستمدة من أجهزة الحاسوب الآلي من المشكلات الإجرائية الهامة، حيث تقف القواعد التقليدية عقبة في سبيل إثبات الجريمة المعلوماتية، فشرط الكتابة في المحرر المكتوب الموقع عليه حتى يكون حجة في الإثبات، قد يكون سببا في عرقلة الاعتراف بحجية الكتابة المدونة على دعامة ممغنطة، في ظل عدم وجود النص القانوني المتضمن الاعتراف بتلك الأدلة المنطقية، وتغيير الحقيقة في محرر، وفقا للطرق التقليدية المنصوص عليها في القوانين كشرط لقيام جريمة التزوير وإثباتها، قد تكون مشكلة بالنسبة للتزوير الناتج عن التلاعب بالبيانات في نظم المعالجة الآلية، لعدم تطابق الوعاء الذي تقع عليه الجريمة[1].

فما هي المشكلات التي تتعلق بالدليل الإلكتروني، وإلى أي مدى يمكن قبول المخرجات الحاسوبية في الإثبات الجنائي؟

1- الدليل الإلكتروني

مع أنه قد أصبح من الضرورة بمكان على السلطات القضائية التعامل مع الأدلة الرقمية، في ظل تكنولوجيات المعلومات واقترانها بتكنولوجيا الاتصالات، وما نتج عنهما في الجانب السلبي من ظهور جرائم لم يكن بعضها معروفا من قبل، والبعض الآخر، وإن كانت معروفة في مسمياتها إلا أنها قد ظهرت مختلفة في تكييفها ووسيلة ارتكابها عن سابقاتها، وظهرت بظهورها أدلة رقمية من نفس نوعية الجريمة، ومن تلك الأدلة ما يعرف ب (ip)، وال (ip addrss).

وال (ip)هو: اختصار لكلمة (internet protacl) بروتوكول الإنترنت، ويعرف بأنه: وسيلة لنقل البيانات من مكان على الإنترنت إلى مكان آخر.

أما (ip addrss) فهو :عنوان مكون من أربعة أرقام، ويستخدم لتحديد هوية كل جهاز يتصل بالإنترنت[2]، ذلك أنه عندما يتجول أي مستخدم للانترنت في حوار إنترنت، فإنه يترك آثاراً في كل موقع قام بزيارته، فأي موقع يقوم بزيارته فإنه يفتح سجلا خاصا

([1]) محمد أبو العلا عقيده، مواجهة الجرائم الناشئة عن استخدام الحاسب الآلي، بحث مقدم إلى مؤتمر حول الكمبيوتر والقانون- ضفاف بحيرة قارون بالفيوم، من 29ينايرالى 1 فبراير 1994م، ص122.

[2] منير الجنبيهي ومحمود الجنبيهي، بروتوكولات وقوانين الإنترنت، مرجع سابق، ص26.

به، يتضمن عنوان الموقع الذي جاء منه، ونوع الكمبيوتر ونوع المتصفح، وعنوان رقم (ip) الدائم، والمتغير للكمبيوتر الذي يتصل منه، كما يمكن في ظروف معينة الحصول على عنوان البريد الالكتروني والاسم الحقيقي عن طريق برامج معينة، ومع ذلك فتوجد مواقع تقدم خدمة إخفاء ال(ip)، بحيث لايتم تسجيله من قبل أي موقع يقوم بزيارته، ومثال ذلك موقع (www.ananymizer.com) حيث سيبدو للموقع الذي يزوره كأنه قادم من عنوان آخر[1]، فهذا الدليل وغيره من الادلة الإلكترونية مازالت محاطة بالعديد من المشكلات أهمها:

أ- طبيعة الدليل في الجرائم المعلوماتية

من المشكلات التي تتعلق بالدليل الإلكتروني أنه دليل غير مرئي، حيث تكون الأدلة الناتجة عن الجرائم المعلوماتية المرتكبة على النظم أو بواسطتها عبارة عن بيانات غير مرئية لا تفصح في الغالب عن شخصية الجاني، وتكون مسجلة الكترونيا، وفي الغالب مشفرة على وسائط تخزين ضوئية أو ممغنطة لا يمكن للإنسان قراءتها، وإن كان ذلك ممكناً للآلة، والتلاعب أو التعديل الذي يحدثه الجاني فيها لا يحدث أثرا، مما يقطع صلة المجرم بالجريمة، ويحول دون كشف شخصيته في الغالب[2]، وبالتالي فإن الطبيعة غير المرئية للأدلة الالكترونية تنعكس سلبا على أداء الجهات التي تتعامل معها، حيث تشكل عملية فحص وتحليل تلك البيانات صعوبة بالغة أمام تلك الجهات التي مازالت الثقافة المادية هي المسيطرة عليها في التعامل مع تلك الأدلة، مع أن الأمر مختلف بالنسبة لهذا النوع من الأدلة الرقمية التي تحتاج إجراءات تتناسب مع طبيعتها غير المرئية .

وتظهر هذه المشكلة على وجه الخصوص بالنسبة لجرائم الإنترنت، ومنها الجرائم التي تقع على العمليات الإلكترونية المختلفة، كالتي تقع على التجارة الإلكترونية، أو على العمليات الإلكترونية للأعمال المصرفية، وقد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، كجرائم السرقة، أو التزوير، أو الإتلاف، أو الغش، وكذلك

---

(1) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2004، ص63، ص64.

(2) Solange Ghernaouti –Hélie, Sécurité Informatique et réseaux, dunod, paris, 2006, P.30.

الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها، إذ يكون من الصعب تحديد مصدر المرسل(1).

ب- قابلية معالم الجريمة للزوال

من الآثار التي ظهرت بظهور الأدلة الرقمية فقدان أكثر الآثار التقليدية التي كانت تعين جهات العدالة الجنائية في كشف الجريمة، والتي كانت تعتمد على المستندات والسجلات المكتوبة، بالرغم من أهميتها في بعض الحالات في كشف الجريمة أكثر من الأدلة الالكترونية التي يتم إخفاؤها (2)

نتيجةً للتعاملات الإلكترونية، فقد يتم في بعض العمليات إدخال البيانات مباشرة في نظام الحاسب الآلي دون تطلب وجود وثائق خاصة بالإدخال، كما هو الحال في نظم العمليات المباشرة التي تقوم على إبدال الإذن الكتابي لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن يتضمنها برنامج الحاسب الآلي.

وبالتالي فإن الأمر الواقع يفرض على السلطات المعنية بالتحري أو التحقيق التعامل مع البيانات المعالجة باعتبارها مستندات الكترونية وفق ضوابط تقنية، ونصوص قانونية.

---

(1) محمود صالح العادلي، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، بحث منشور في منتدى قوانين قطر، وملف ورد على الموقع الأخر، وموقع منتدى الشروق أو لاين ،تم التأكد من أن البحث مازال متاح في المواقع المشار إليها في 10/1 /2009على الروابط :

http://www.law-zag.com/vb/showthread.php?s=db2dfbed90fe7d5cb217bee924b47901&p=33245#post33245
http://www.ituarabic.org/coe/2006/E-Crime/Documents%20and%20Presentations/DAY%201/Doc7-Om.PPT
http://www.echoroukonline.com/montada/showthread.php?t=7916

(2) وكمثال لأهمية الدليل التقليدي في الكشف عن الجريمة أكثر من الآثار الإلكترونية، ما حدث في ألمانيا الاتحادية من قيام مبرمجي أنظمة في جهة عملهم من وضع اسم لشركة وهمية بدلا عن اسم الشركة الموردة لجهة عملهم على ملف البيانات الرئيسي الذي يربط أرقام الحسابات بعناوين الموردين بغرض مراجعة الفواتير، ونتيجة لذلك التعديل فقد اصدر الحاسب الفاتورة باسم الشركة الوهمية، إلا أن الشيك - بمبلغ 135181 مارك ألماني – إذ كان لمورد غير معروف، فقد آثار الشك وتم وقف صرفه، ولم يكن التحقيق وتتبع الآثار الإلكترونية في ملف التشغيل من خلال تحليل الملف مجديا نظرا لاختفاء تسجيلات التشغيل بفترات معينة حيث تعذر اكتشاف الشخص الذي أدخل التغيرات، وبالتالي لم تفلح الآثار الإلكترونية في الكشف عن الجريمة، وتم اكتشافها بواسطة أدلة تقليدية، من خلال رسالة أتت من البنك الذي فتح الجناة حسابا فيه باسم الشركة الوهمية إلى صندوق بريد الشركة، ومع أنه لم يتم اكتشافهم من خلال الصندوق البريدي، كونهم وضعوا عنوانه جوار صندوق بريد لمنزل كبير، ولم يترددوا عليه لأخذ الشيك حتى لا يكتشف أمرهم، فقد تم اكتشافهم بعد مقارنة خطوط الموظفين بالخط الموجود في استمارات البنك بغرض فتح الرصيد. لمزيد من التفصيل راجع: هشام محمد فريد رستم، أصول التحقيق الجنائي الفني في جرائم الحاسوب، مرجع سابق، ص426، وص427.

كما أنه في بعض العمليات المالية قد يجري الحاسب بعض العمليات المحاسبية بغير حاجة إلى إدخال، كما هو الحال في احتساب الفوائد في الإيداعات البنكية، وقيدها آليا بأرصدة العملاء على أساس الشروط المتفق عليها مسبقا والموجودة في برنامج الحاسب الآلي، وفي العمليات المشار إليها قد يتم ارتكاب العديد من الجرائم، كاختلاس المال والتزوير بإدخال بيانات غير معتمده في نظام الحاسب، أو تعديل برامجه، أو البيانات المخزنة بداخله دون ترك ما يشير إلى حدوث الإدخال أو التعديل.

ج- سهولة محو الدليل

كذلك فإن من المشكلات التي تتعلق بالدليل الإلكتروني سهولة محوه من قبل الجاني، حيث يستطيع الجاني أن يمحو الدليل الالكتروني، إما من خلال برنامج يتضمن أوامر بإتلاف الملفات في حال محاولة التفتيش عليها من قبل الجهات المعنية، أو بأي وسيلة تقنية أخرى، وإرجاع تفسير ذلك العمل في بعض الحالات إلى خطأ في نظام الحاسب أو الشبكة [1].

ومع أن مسألة الإتلاف المعلوماتي يمكن إثباتها حسب رأى البعض من خلال تشغيل الجهاز، ورؤية ما تم حدوثه من تدمير للبيانات، أو محوها، أو إدخال بيانات غير أصلية عليها، باستثناء مسألة الإثبات بالنسبة لسرقة المعلومات، حيث يصعب إثباتها حسب هذا الرأي [2]، فإنه يبدو بأن مسألة إثبات الإتلاف المعلوماتي مثلها مثل باقي الجرائم المعلوماتية مازالت مسألة معقدة إلى درجة كبيرة في ظل عدم وجود التخصص الفني الدقيق للأجهزة المعنية بالإثبات، والبعد الدولي للجريمة التي أضحت عابرة للحدود الجغرافية، بحيث لا يتقيد ارتكابها بمكان ما.

فجريمة الإتلاف وإن كان بالإمكان معرفتها من خلال البرامج المتلفة، أو الأنظمة التي تعرضت للعطب، وكذلك البيانات المخزنة في نظام المعالجة الآلية للبيانات، إلا أنها

---

(1) ومن تلك القضايا ما حدث مؤخرا في النمسا من قيام أحد مهربي الأسلحة بإدخال تعديلات على نظام حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين معه، بحيث يترتب على إدخال أمر على الحاسب من خلال لوحة المفاتيح بالنسخ أو الطبع، إلغاء كافة البيانات وتدميرها، وكان ذلك بهدف الحيلولة دون نجاح أجهزة الملاحقة في إجراءاتها الخاصة في البحث عن الأدلة وضبطها، لولا تنبه المختصين بحدوث شيء ما في جهاز الفاعل، ومن ثم قيامهم باستنساخ الأقراص الممغنطة التي تم ضبطها بواسطة أنظمتهم. راجع: هشام محمد فريد رستم، أصول التحقيق الجنائي في جرائم الحاسوب، مرجع سابق، ص430 .

(2) هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الالكتروني ،ج 2،بحث قُدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الحقوق ،جامعة الإمارات العربية المتحدة، 2000، ص903.

في مجال الإثبات تواجه ذات المعوقات التي تواجهها الجرائم الأخرى في مجال المعلوماتية .

د- صعوبة استخراج الدليل من البيانات الضخمة

تعد إحدى المشكلات التي تتعلق بالدليل الإلكتروني، ضخامة البيانات المتعين فحصها للوصول إلى الدليل، مقابل نقص خبرة الجهات المختصة في الاستدلال أو التحقيق أو المحاكمة، حيث تعد ضخامة البيانات المتعين فحصها إثر جريمة ارتكبت من أهم المشكلات التي تعيق الحصول على الدليل، ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لحاسب متوسط يتطلب آلاف الصفحات التي قد لا تثبت شيئا يفيد الواقعة على الإطلاق، إذ أن المحقق غير المدرب قد يحجز بيانات تفوق القدرة البشرية على مراجعتها، أو يتغاضى عنها كليا ويحاول الحصول على أدلة تقليدية من المتهم، وقد لا يكون أمام سلطات العدلية القضائية إزاء ذلك إلا أحد أمرين [1]:

الأول: الاستعانة بالبرامج وما تتيحه وسائل المعالجة الآلية للبيانات من أساليب التدقيق والفحص المنظم أو المنهجي، وذلك يتطلب أن يكون القائم على عملية الفحص مدربا وملما بتلك الوسائل والأساليب، وتكون الدول المتقدمة هي السباقة في إيجاد جهات متخصصة ومدربة في مجال مكافحة وضبط الإجرام المعلوماتي.

والثاني:الاستعانة بخبير نظرا للطابع الفني الخاص بارتكاب الجرائم المتعلقة بتكنولوجيا المعلومات، والطبيعة غير المادية لمحل الاعتداء، وبهذا الشأن فقد يكون الخبير هو من يحدد طبيعة المهمة وحدودها، وذلك غير مرغوب فيه، لكون دور الخبير سيطغى على دور المحقق أو القاضي الذي ينقصه الإلمام بالجوانب التقنية للجريمة مع أنه صاحب القرار أو الحكم في المسألة، وبالتالي فإن العبارة التي مفادها **"**أن القاضي هو خبير الخبراء**"** ستصبح عديمة الجدوى.

بالإضافة إلا أن الخبير قد يهدف إلى تحقيق مصلحته الشخصية لا المصلحة العامة للمجتمع، وقد يتخذ إجراءات تقنية تخدم براءة المتهم، خلافا لما تقتضيه أعمال الخبرة في كشف الحقيقة، دون أن يتنبه المحقق أو القاضي لذلك، بسبب عدم وجود حد أدنى من الإلمام في ذات المجال.

([1]) هشام محمد فريد رستم، أصول التحقيق الجنائي في جرائم الحاسوب، مرجع سابق، ص430، و ص432.

هـ - عرقلة الوصول إلى الدليل

بالرغم من قيام العديد من الجهات بتوفير الحماية الأمنية للمعلومات والبرامج المخزنة بالأنظمة المعلوماتية التابعة لها عن طريق الأنظمة الأمنية، وما تتبعه من وسائل باستخدام التشفير والترميز وغيرها من طرق الحماية، إلا أن ذلك لا يحول دون اختراق تلك الأنظمة من قبل قراصنة الحاسب الآلي، وعلى وجه الخصوص العاملين في ذات المؤسسات التي تم اختراق أنظمتها، ومن ثم فإن تلك الحماية تصبح عديمة الجدوى، حيث يعمد أولئك إلى الدخول إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها أو استخدامها في مؤسسات تجارية يسعون لإنشائها، أو يكون هدفهم فقط تخريب المعلومات عن طريق تغيير الأرقام والبيانات، بل إن هؤلاء يقومون بفرض تدابير أمنية تحول دون الوصول إلى الأدلة التي يمكن ضبطها ضدهم باستخدام كلمات سر حول مواقعهم تمنع الوصول إليها، أو ترميزها أو تشفيرها لإعاقة الاطلاع على أي دليل يخلفه نشاطهم الإجرامي (1).

كذلك فإن من معوقات الوصول إلى الدليل يتمثل في حال أن تكون تلك البيانات التي لها علاقة بالجريمة محل البحث مخزنة خارج الدولة عن طريق شبكة الإنترنت، ففي مثل هذه الحالة فإن البحث عن الأدلة يتعارض مع مبدأ السيادة التي تحرص عليه كل دولة، وبالتالي فلن يتم التوصل إلى الدليل مالم يوجد تعاون دولي بهذا الخصوص(2).

ه- كذلك فإن من المشكلات التي تتعلق بالدليل الالكتروني وتعيق الوصول إليه، هو أن عددا كبيرا من الأشخاص قد يترددوا على مسرح الجريمة خلال الفترة الزمنية التي تتوسط ارتكابها واكتشافها مما يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالأدلة، أو زوالها أو بعضها وذلك ما يثير الشك في الدليل الالكتروني المتحصل عليه (3).

---

(1)راجع: عبد الفتاح بيومي حجازي، مرجع سابق، ص51.

(2) علي محمود حمود: الأدلة الإلكترونية المتحصلة من الإثبات الإلكتروني في ظل الإثبات الجنائي، بحث تم تقديمه إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، من 26 – 28 نيسان 2003،منشور على موقع كلية الحقوق جامعة المنصورة، س.د 11 bm ،ت.د 2009/4/8،على الرابط:

Http://www.f-law.net/law/shozthread.php?t=1133

(3) عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، مرجع سابق، ص365، وص366.

2- مدى قبول حجية الدليل الإلكتروني في الإثبات

الحجية هي: الاستدلال على صدق الدعوى أو كذبها، وهي تعني البينة، وحجية المخرجات الكمبيوترية هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، ويقصد بها قيمة ما يتمتع به المخرج الكمبيوتري بأنواعه المختلفة سواء كانت ورقية أم إلكترونية أم مصغرات فلميه من قوة استدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه [1].

ومع أن الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جداً فيما تحتويه من معلومات، مثل صفحات المواقع المختلفة Web) (Pages والبريد الإلكتروني (Email E، والفيديو الرقمي (digital) Video)، والصوت الرقمي (Digital audio) ، وغرف الدردشة والمحادثة Digital Logs) of Synchronous Chat Sessions)، والملفات المخزنة في الكمبيوتر الشخصي (Files Stored On Personal Computer)، والصورة المرئية Digitized) (Still Images، والدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات (Computer Logs from An Internet (service (I S P) Provider [2]، إلا أنها مازالت محلا لخلاف فقهي حول مدى حجيتها في الإثبات، ذلك أن الخلاف مازال قائما بين الاتجاهات الفقهية حول مدى حجية الدليل التقليدي في الإثبات، وفقا لمبدأ قناعة القاضي من مبدأ الدليل القانوني.

فحجية الدليل الإلكتروني في الإثبات تعترضه العديد من المشكلات التي تثير مدى حجيته في الإثبات ويترتب على ذلك وجود خلاف فقهي حول حجية الدليل الالكتروني بحسب الفقه المقارن فيما إذا كان لاتينيا، أو أنجلو سكسونيا، أو مختلطا، كما أن من المشكلات التي أثيرت في حجية الدليل الإلكتروني تتمثل في ما مدى اعتماد برتوكول TCP/IPكدليل رقمي ذي حجية قضائية.

---

(1) مروك نصر الدين، محاضرات في الإثبات الجنائي، ج2، دار هومة، الجزائر، 2004، ص461.

(2) راجع ممدوح عبد الحميد عبد المطلب: استخدام بروتوكول (Tcp/ip)في بحث وتحقيق الجرائم على الكمبيوتر، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية،أكاديمية شرطة دبي - الإمارات العربية المتحدة، 26 :28نيسان 2003، منشور في شبكة الإنترنت، موقع كلية الحقوق ،جامعة المنصورة، ت .د 2009/8/28على الرابط :
http://www.f-law.net/law/showthread.php?p=79241

أ- **المنازعة في حجية الدليل الالكتروني**

إضافة إلى المشكلات التي تثيرها الأدلة الإلكترونية والمتعلقة بطبيعتها المعنوية، يوجد عدد من المشكلات التي تتعلق بحجية تلك الأدلة في الإثبات وتثار خلافات بسببها ومنها:

1) قبول الأدلة المتحصلة عن الوسائل الإلكترونية

تثير الأدلة المتحصلة من الوسائل الإلكترونية مشكلة مدى قبول تسجيلات ومخرجات الحاسب الآلي كأدلة إثبات جنائي، ذلك أن الطبيعة الخاصة التي تتميز بها الأدلة الرقمية، وما يصاحب الحصول عليها من خطوات معقدة، يجعل من قبول حجيتها مشكلة أمام القضاء، وبالتالي فقد ذهبت العديد من التشريعات المقارنة - بهدف تلافي تلك المشكلة - إلى إقرار قبول مصادر المعلومات الخاصة بالحاسوب أو المتحصل عليها من أنظمته، مثل مخرجات نظام المعالجة الآلية للبيانات، والبيانات المكتوبة على شاشته، والبيانات المسجلة على دعائم ممغنطة أو المخزنة داخل نظام المعالجة الآلية للبيانات، كأدلة يقوم عليها الإثبات الجنائي، إضافة إلى تقرير حق القاضي في تقدير الدليل[1].

2) حدود الأدلة العلمية والأدلة الرقمية

الوسائل العلمية بما فيها الإلكترونية وإن كانت تفيد في تسهيل مهمة كشف الحقيقة، إلا أنها قد تعصف بحقوق وحريات الأفراد في حالة سوء استخدامها، وقد تمس أدق خصوصيات الإنسان، ولذلك يتطلب الأمر معياراً مزدوجاً لقبول الدليل العلمي، فمن ناحية يجب أن تصل قيمة الدليل العلمي إلى درجة القطع من الناحية العلمية البحتة، ومن ناحية ثانية: ألا يكون في الأخذ بهذا الدليل مساس بحقوق وحريات الأفراد إلا بالقدر المسموح به قانونا[2].

3) ومن المسائل الخلافية التي تثيرها حجية الدليل الالكتروني في الإثبات هي مدى جواز إجبار الشاهد على الإدلاء بكلمة السر اللازمة للدخول إلى المعلومات المجرمة

---

(1) علي محمود حمود، مرجع سابق منشور على شبكة الإنترنت على الرابط:
Http://www.f-law.net/law/shozthread.php?t=1133

وراجع أيضا:
Solange Ghernaouti –Hélie, Sécurité Informatique et réseaux, dunod, paris, 2006, P.30.

(2) جميل عبد الباقي الصغير أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص47.

أو الإطلاع على الملفات السرية المخزنة في نظام الحاسوب، أو فك الشفرة الخاصة بالبرامج التشغيلية .

وبهذا الصدد فقد وجد خلاف في الفقه المقارن بين مؤيد ومعارض، فبينما ذهب اتجاه : إلى أنه ليس من واجب الشاهد - وفقا للالتزامات التقليدية للشهادة- أن يقوم بما تم ذكره، وبالتالي يكون من الصعب إجباره على تقديم بيانات يجهلها ولم يقم بإدخالها بنفسه في ذاكرة الحاسوب، وإن كان يستطيع الوصول إليها، نظرا لمعرفته بكلمة المرور السرية (1).

بينما ذهب أصحاب الاتجاه الأخر: إلى أن من الالتزامات التي يقوم بها الشاهد هي طبع ملفات البيانات، أو الإفصاح عن كلمة السر أو الشفرات الخاصة بالبرامج المختلفة(2).

ب- مدى اقتناع الأنظمة القضائية بحجية الدليل الالكتروني في الإثبات

تكمن صعوبة الاستناد إلى الدليل الإلكتروني في الإثبات في سهولة تعديل البيانات التي يحتويها، كما توجد صعوبات أخرى مردها أن الدليل الإلكتروني قد يكون صادراً من جهاز المجني عليه (3).

وتختلف حجية الدليل في النظام اللاتيني، عنه في النظام ألا نجلو سكسوني، عنه في النظام المختلط، وقد تمثل حجية الدليل الإلكتروني صعوبة اكبر في مدى قبوله، ذلك أن المشكلة القانونية المطروحة بهذا الخصوص تتمثل في مدى جواز اعتماد القاضي في

---

(1) تضمنت العديد من التشريعات حماية الشاهد من الإدلاء بمعلومات عن كلمة السر أو عن الملفات المخزنة، ففي لوكسمبورغ فإن الشاهد ليس مجبرا على التعاون في كل ما يعرفه عند سؤاله أمام المحكمة، وفي ألمانيا تذهب غالبية الفقه بعدم إلزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسوب،على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وفي تركيا لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمة المرور السرية، أو كشف شفرات تشغيل البرامج المختلفة. راجع على حسن محمد الطوالبة، مرجع سابق، ص186.

(2)ففي فرنسا يرى جانب من الفقه أنه في حالة غياب النص التشريعي، يكون الشاهد مكلفا بالكشف عن كلمة المرور السرية التي يعرفها وشفرات تشغيل البرامج، باستثناء المحافظة على سر المهنة، وفي هولندا يتيح قانون الحاسوب لسلطات التحقيق إصدار أمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح بكلمات المرور السرية، والشفرات الخاصة بتشغيل البرامج المختلفة، كذلك القانون الإنجليزي الصادر في عام 1984 في شأن الأدلة الجنائية حيث يفرض على الشاهد بأن يقدم إلى العدالة ما يعرفه من معلومات يتضمنها جهاز الكمبيوتر،

وكذلك المادة (125) إ.ج هولندي والتي بموجبها يلزم الشاهد بالتعاون مع سلطة التحقيق في مجال الجريمة المعلوماتية، ومن القوانين التي ألزمت مزودي الخدمات بالكشف عن المعلومات والتعاون مع الجهات القضائية ق.إ.ج الهولندي بموجب نص المادة (138).راجع علي حسن محمد الطوالبة، المرجع السابق، ص187، شيماء عبد الغني محمد عطا الله، مرجع سابق، ص437 .

(3) شيماء عبد الغني محمد عطا الله، مرجع سابق، ص479.

تكوين عقيدته على مستخرج من جهاز يمكن التلاعب فيه بالإضافة، أو الحذف، أو التعديل.

1) حجية الدليل الإلكتروني في النظام اللاتيني

تشمل القوانين ذات الصياغة اللاتينية القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الايطالي والاسباني وقوانين أمريكا اللاتينية، كما تشمل القانون الألماني ذلك أن القانون الألماني وإن لم يكن لاتيني النزعة إلا انه يتشابه في صياغته مع القانون الفرنسي، وكذلك القوانين المتأثرة بالنزعة الاشتراكية الحديثة كالقانون الصيني لأنها قريبة من صياغة القانون الفرنسي، فهذه القوانين تتشابه في الصياغة، حيث تكاد تكون مصادرها واحدة، وأصولها العامة متحدة، وتقسيماتها متماثلة، والاصطلاحات القانونية فيها متشابهة [1].

والإثبات في هذه القوانين – اللاتينية- يتبع نظام الإثبات الحر، إذ أن الإثبات في هذا النظام لا يرسم طريق محددة يتبعها القاضي، بل يترك حرية تقدير أدلة الإثبات للقاضي، وفقا لمبدأ حرية القاضي في الاقتناع فالقاضي له كامل الحرية في تقدير قيمة الأدلة المعروضة عليه تقديرا منطقيا [2].

وهذا المبدأ يبدو أكثر شمولا في القانون الفرنسي حيث نصت عليه المادة (310) إ.ج.ف والتي بموجبها أسندت للقاضي سلطة تفويضية تسمح له في باللجوء إلى كل الإجراءات المفيدة لإظهار الحقيقة [3].

---

(1)هلالي عبد اللاه أحمد، حجية المستخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص29.

(2)هلالي عبد اللاه أحمد، المرجع السابق، ص34. مروك نصر الدين، مرجع سابق، ص467.

(3) **Article 310**

(Loi nº 72-1226 du 29 décembre 1972 art. 6-i, 6-ii Journal Officiel du 30 décembre 1972 en vigueur le 1er janvier 1973)

Le président est investi d'un pouvoir discrétionnaire en vertu duquel il peut, en son honneur et en sa conscience, prendre toutes mesures qu'il croit utiles pour découvrir la vérité. Il peut, s'il l'estime opportun, saisir la cour qui statue dans les conditions prévues à l'article 316.

Il peut au cours des débats appeler, au besoin par mandat d'amener, et entendre toutes personnes ou se faire apporter toutes nouvelles pièces qui lui paraissent, d'après les développements donnés à l'audience, utiles à la manifestation de la vérité.

Les témoins ainsi appelés ne prêtent pas serment et leurs déclarations ne sont considérées que comme renseignements.

للاطلاع على النص بالفرنسي انظر ،شبكة الإنترنت، ت.د 2009/2/25 على الرابط :

http://www.legislationline.org/documents/section/criminal-codes

ويترتب على الأخذ بهذا النظام أن حجية الدليل الإلكتروني في الإثبات لا تثير صعوبات في تقديم هذه الأدلة لإثبات الجرائم المعلوماتية، فالقاضي يمتلك الحرية في الأخذ بهذه الأدلة، وتكوين عقيدته بموجبها، بحيث لا يخضع في ذلك لرقابة محكمة النقض في تقديره الشخصي لتلك الأدلة، والرقابة التي توجد على القاضي بهذا الخصوص هي رقابة موضوعية تتعلق بالجانب الموضوعي، وتكمن في الرقابة على المبررات التي جعلته يأخذ بتلك الأدلة، وقد أخذت بذلك العديد من التشريعات[1]، وتشترط بعض هذه الدول في أن يكون الدليل الإلكتروني مقروءا، سواء كان مطبوعا بعد خروجه من الجهاز أم كان مقروءاً من خلال شاشة الجهاز نفسه[2]، ومن التطبيقات القضائية على ذلك[3]

2) حجية الدليل الإلكتروني في النظام الأ نجلو سكسوني

حجية الدليل الإلكتروني في النظام الأنجلوسكسوني تعتمد على تقدير المشرع للأدلة وليس لتقدير القاضي، فالدول التي تأخذ بهذا النظام- وعلى رأسها بريطانيا وكندا واستراليا، وجنوب إفريقيا – تطلب شروطا خاصة في الأدلة بوجه عام، حتى يتم الأخذ بتلك الأدلة [4].

والقاضي وفقا لهذا النظام مقيد بالدليل وفقا للضوابط القانونية حتى يتمكن من العمل بدليل ما واعتباره حجة، وبالتالي فهو لا يستطيع أن يحكم بالإدانة، بل يحكم باستبعاد الدليل حتى لو اقتنع بأن المتهم مدان، بمعنى أنه لا يستطيع أن يتحرى الحقيقة بطرق أخرى، بموجب اقتناعه بذلك الدليل، باعتباره حجة، ما لم ينص عليه القانون[5].

(1) ومن تلك الدول لوكسمبورج والتي اعتبرت أن مبدأ الاقتناع الذاتي للقاضي هو حجر الزاوية في الأحكام الجنائية، وفي تركيا ينبسط نطاق الأدلة المعنوية ليشمل إثبات الجرائم المرتكبة عن طريق المعلوماتية، وكذلك في ألمانيا واليونان، والبرازيل، والنمسا، وسويسرا، والنرويج. راجع : هلالي عبد أللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي، القاهرة، 2002، ص43 وما بعدها.

(2) ومن الدول التي اشترطت أن يكون الدليل الإلكتروني مقروء اليونان، والبرازيل، والنمسا، وسويسرا، والنرويج. راجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص479 .

(3) ما قضت به محكمة النقض الفرنسية من" أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي" راجع على حسن محمد الطوالبة، مرجع سابق، ص 196، وهلالي عبداللاه أحمد، مرجع سابق، ص43.

(4) شيماء عبد الغني محمد عطا الله، مرجع سابق، ص479.

(5) راجع هلالي عبد أللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص50.

ويترتب على ذلك أن هذا النظام – المقيد للإثبات- يتعارض مع الإثبات في مجال الكمبيوتر والإنترنت، وذلك ما يستدعي إدخال تعديلات تتلاءم مع طبيعة تلك الجرائم، حيث رفض القضاء في بعض الدول العمل بتلك الأدلة[1].

بيد أنه قد طرأت بعض التغييرات على حدة هذا لنظام، فالقانون العام في إنجلترا لم يعد يأخذ بنظرية الأدلة القانونية على إطلاقها[2]، بل أضحى يقبل بمبدأ حرية تقدير الأدلة، إذ أن مبدأ حرية القاضي في تقدير الدليل قد أصبح معترفا به في جميع الأنظمة، فهو في الأنظمة ذات الصياغة اللاتينية يعبر عنه بعبارة "الاقتناع الذاتي " وفي بلاد القانون العام يتحدثون عن "الإدانة بدون أي شك معقول أو أدنى شك".

ومع أن القانون الانجليزي لا ينظر إلى الأدلة الناتجة عن الآلات على أنها من قبيل الشهادة السماعية، إلا أنها قد أصبحت مقبولة في الإثبات في المواد الجنائية، وبالتالي فإن لقطات الكيمرا المأخوذة للمتهم أثناء ارتكابه للجريمة، أصبحت مقبولة في إثبات الجريمة[3].

وخلاصة ذلك أن العمل بتقدير القاضي للدليل معمول به في كل الأنظمة إلا أنه في القوانين ذات الصياغة الأنجلوسكسونية يكون الإثبات فيها ابعد من أن يكون إثباتا قانونيا

([1]) ومن تلك الدول التي رفض قضائها العمل بالأدلة غير القانونية بريطانيا حيث تم رفض الاعتداد بالميكروفيلم كدليل في المواد الجنائية، وقد قضت بذلك محكمة اللوردات في قضية (Myers contre) .راجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص465.

([2]) وتطبيقا لكون القضاء الأنجلوسكسوني قد تغيرت نظرته من العمل بالدليل القانوني الذي مصدره القانون فحسب دون أن يترك سلطة تقديرية لقاضي في تقدير حجية دليل الإثبات :

- في إحدى القضايا في بريطانيا تم الاعتداد بالدليل المستخرج من الحاسوب التابع للمجني عليه، والمتمثل في تركيبة المادة الكيمائية التي سرقت عليه، حيث تم اعتبار الورقة المستخرجة من جهاز الحاسوب الخاص بالمجني عليه مقبولة، وفقا للشريعة العامة وتختلف عن الشهادة السمعية.
- كما قبلت المحكمة الجزائية في بريطانيا بالدليل المستخرج من جهاز الحاسوب في قضية R.v.pettigrew بوصفه شهادة مباشرة، وليست سماعية، والتي تخلص وقائعها في أنه وجد في حيازة المتهم الذي قام بالسطو على البنك أرقام نقود من التي كانت مسجلة في كمبيوتر البنك في انجلترا، حيث قبلت المحكمة الأدلة الورقية المستخرجة من جهاز الحاسوب، باعتبارها دليلا مباشرا وليس من الأدلة السمعية.
- وبخصوص التسجيلات الممغنطة في الإثبات فقد نظمت بعض التشريعات ذلك ومنها القانون المدني لمقاطعة الكيبيك بكندا في المادة رقم(2874) والتي يسمح بموجبها بقبول التسجيلات على شرائط ممغنطة كدليل في الإثبات إذا توافرت شروط ثلاثة هي: أن تكون التكنولوجيا المستخدمة في التسجيلات موثوق بها، وان يتم إثبات التسجيل بطريقة غير الشريط الممغنط كشهادة احد الأشخاص بأن هذا الإقرار المتواجد في الشريط هو إقرار المتهم، وأن تكون الإقرارات المسجلة على الشريط واضحة ومفهومة ومحددة لهوية صاحبها، فإذا اجتمعت الشروط الثلاثة في التسجيل كان له قوة الإثبات. راجع: شيماء عبد الغني محمد عطاء الله، المرجع السابق، ص337.

([3]) شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، مرجع سابق، ص475.

أو مقيدا، وأدنى إلى أن يكون إثباتا مختلطا[1]، ومع ذلك فإن نظام الأدلة القانونية يظل هو السائد في الأنظمة الأنجلوسكسونية، لذلك فإن حجية المخرجات الكمبيوترية تجد بعض الصعوبات التي تواجهها كأدلة في الإثبات.

3) حجية الدليل الإلكتروني في النظام المختلط

في القوانين ذات الاتجاه المختلط يتم الجمع بين النظامين اللاتيني والأنجلوسكسوني، فالنظام المختلط عبارة عن محاولة توفيقية بين النظامين السابقين، لتلافي السلبيات التي وجهت إلى النظام اللاتيني والمتمثلة في احتمال تعسف القاضي من خلال سلطته التقديرية في الاقتناع بالدليل من عدمه، وكذلك تلافي سلبيات النظام الأنجلوسكسوني التي من خلالها يكون دور القاضي سلبيا في عملية الإثبات، وذلك بتقيده بالأدلة القانونية.

وقد يكون التوفيق بين النظامين عندما يحدد القانون أدلة معينة للإثبات في بعض الوقائع دون الأخرى، أو يشترط في الدليل شروطا في بعض الأحوال[2]، أو يعطي القاضي الحرية في تقدير الأدلة القانونية مثل القانون الياباني حيث حصر طرق الإثبات المقبولة بأقوال المتهم، و أقوال الشهود، والقرائن والخبرة.

أما بالنسبة لأدلة الحاسوب والإنترنت فيقرر البعض أن السجلات الإلكترونية تكون غير مرئية في حد ذاتها، لذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي هذه الحالة يتم قبول المخرجات الناتجة عن الحاسوب والإنترنت سواءً كانت هي الأصل أم كانت نسخة من الأصل.

كذلك يرى آخرون أن الدليل الناتج عن الحاسوب يمكن أن يكون مقبولا في المحكمة كدليل كتابي أو مستندي، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات، ومنها التصوير الفوتغرافي، والتصوير بالأقمار الصناعية، فهذه الوسائل

---

(1) هلالي عبد اللاه أحمد،حجية المخرجات الكمبيوترية في الإثبات الجنائي، مرجع سابق، ص 52.
(2)هلالي عبد اللاه أحمد، حجية المستخرجات الكمبيوترية في الإثبات الجنائي، مرجع سابق، ص59.

العلمية يمكن اعتبارها مستندات بالمعنى الواسع، ذلك أن التقدم الفني قد تجاوز المفهوم التقليدي للمستند الذي يعرفه أنه مجرد ورقة مكتوبة[1].

ج- مدى اعتماد برتوكول TCP/IP كدليل رقمي ذي حجية قضائية

لقد تم التركيز من خلال هذا الموضع المتعلق بحجية الدليل الالكتروني في الإثبات على دراسة مدى حجية بروتوكول (TCP/IP) في الإثبات الجنائي لكونهما من أكثر البروتوكولات المستخدمة في شبكات الإنترنت، فهي جزء أساسي منه، ولما لأهمية الاستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها هذا البروتوكول في تحقيق جرائم الكمبيوتر، حيث إنها تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة، وتحديد الأجهزة التي أصابها الضرر من الفعل الإجرامي، وتحديد نوعية النشاط الإجرامي خلال الفترة الزمنية، ولأنهما يستخدمان تقنية التبادل المعلوماتي بواسطة الحزم المعلوماتية بين مختلف أجهزة الكمبيوتر المتصلة بالشبكة المعلوماتية؛ ويقدمان أسلوباً علمياً وقانونياً، يمكن الاستعانة به في إثبات الجريمة التي تتم عبر أجهزة الكمبيوتر، كما أنهما يساعدان على بلورة فهم الدليل الرقمي المقدم لأجهزة إنفاذ وتطبيق القانون[2].

وبهذا الشأن يعتبر بعض الفقهاء أنه يمكن الاعتماد على (IP)، و(T c p) كأدلة في الإثبات الجنائي، ذلك أن هذا البروتوكول (IP) يعتبر وسيلة لنقل البيانات من مكان على الإنترنت إلى مكان أخر، ويستخدم لتحديد هوية كل جهاز على الإنترنت، حيث

---

(1) وينسب الرأي الأول إلى الفقه الياباني بينما ينسب الأخر إلى الفقه الشيلي . راجع: هلالي عبد اللاه أحمد، المرجع السابق، ص64،ص65. وعلى حسن الطوالبه، مرجع سابق، ص198.

(2) يعرف الدليل الرقمي بأنه الدليل المأخوذ من جهاز الكمبيوتر، و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وبروتوكول (Tcp/Ip) اختصار ل (Transmission Control Protocol، Internet Protocol) وهي عائلة بروتوكولات الاتصالات بين عدة أجهزة من الكمبيوتر طورت أساساً لنقل البيانات بين أنظمة (U N I X) ثم أصبحت المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الإنترنت بواسطة الاتصال الهاتفي، وبروتوكول (TCP/IP) يضم في الواقع بروتوكولين مستقلين في شبكة الإنترنت، هما بروتوكول (TCP)وبروتوكول (IP) حيث يعملان معاً وبشكل متزامن،ويرتكز البروتوكولان معاً على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Packet) بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها، وحزمة المعلومات هي جزء أو قسم من ملف معلوماتي ذات حجم مصغر ثابت،تحمل كل منها رقماً خاصاً ومعلومات تعريفية بكل من المرسل والمرسل إليه، بحيث تعبر كل حزمة عبر شبكة الإنترنت بشكل مستقل ويتراوح حجم الحزمة من 40 و 32.000 بايت (بمعدل متوسط قدره 1500 بايت) وعند كل وصلة، تتم قراءة جهة المقصد أو المرسل إليه، ثم تتم إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد النهائية. راجع: ممدوح عبد الحميد عبد المطلب: استخدام بروتوكول (IP/TCP) في بحث و تحقيق جرائم الحاسوب، مرجع سابق.
http://www.f-law.net/law/showthread.php?p=7924

يمكن الاستفادة حول ما يكشف عنه رقم (IP) من معرفة جهاز الكمبيوتر الذي تم الاتصال منه، وكذا معرفة عنوان مرسل الرسالة الإلكترونية، بل إن المرسل إليه الرسالة يستطيع معرفة عنوان المرسل من خلال استخدام برنامج (اللاوت لوك) بعد النقر على(option) [1].

وبالرجوع إلى نصوص القانون اليمني والجزائري لمعرفة النظام المتبع في التعامل مع الأدلة وحجيتها في الإثبات، يلاحظ بأنهما قد سارا على نهج النظام اللاتيني في الإثبات والذي يترك للقاضي حرية تقدير الدليل، حيث خول القانون اليمني للقاضي أن يحكم في الدعوى بمقتضى العقيدة التي تكونت لديه بكامل حريته[2]، وكذلك القانون الجزائري[3].

ومع أن قانون الإجراءات الجزائية اليمني عندما ذكر أنواع أدلة الإثبات في الدعوى الجزائية قد أشار إلى أنها أدلة مادية ملموسة[4]، وإن جعل تقديرها وفقا لاقتناع المحكمة، وتتمثل تلك الأدلة بشهادة الشهود، وتقرير الخبراء، واعتراف المتهم، والمستندات بما فيها أية تقارير رسمية مرتبطة بشخصية المتهم أو وقائع الجريمة والقرائن والأدلة الأخرى، إلا أنه ومن خلال بعض نصوص القانون اليمني رقم (40) لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية يمكن الخروج بنتيجة مفادها، أن المشرع اليمني - من خلال هذا القانون- قد خول للسلطات المختصة الاعتماد على الدليل الإلكتروني واعتباره حجة في الإثبات، وإن كان ذلك في مجال المعاملات المالية والمصرفية [5]، فلا يوجد ما يمنع من تطبيق ذلك على الأدلة الإلكترونية في مجال كشف

([1])عبد الفتاح بيومي حجازي، مرجع سابق، ص64.

([2]) راجع: المادة (367) إ.ج.ي. ، وراجع: حسن علي مجلي، المحاكمة في قانون الإجراءات الجزائية اليمني، بدون ذكر دار النشر ورقم الطبعة، 2001،ص99.

([3]) راجع: المادة (212) إ.ج.ج .

(4) نصت المادة (340) إ.ج. ي على أن : (الأدلة المادية هي أشياء بحكم تكونها وذاتيتها أوصلتها بالواقعة محل البحث تمكن من إجراء استنتاجات حول الجريمة وأسبابها وظروفها، وحول المتهم كأداة الجريمة والشيء المحتفظ بأثر من آثارها، والنقود وغيرها من القيم المتحصله من الجريمة، وتقدم الأدلة المادية أثناء المحاكمة وإذا استحال ذلك بسبب طبيعة الشيء وجب إعداد الصور والرسوم وإلحاقها بالملف)

([5]) أصدر المشرع اليمني القانون رقم (40) لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وجعل نطاق سريانه بموجب نص المادة(4) على جميع المعاملات الإلكترونية التي تضمنها، والتي هي عبارة عن كيانات منطقية أظهرها التقدم التكنولوجي وأصبح التعامل بها تقتضيه حالة الضرورة، ومن ثم لابد من الاعتراف بها وبحجيتها في الإثبات، ومنها رسائل البيانات والمعلومات الإلكترونية وتبادلها، والسجلات الإلكترونية، والتوقيع الإلكتروني، والترميز والتوثيق الإلكتروني.

كما نصت المادة (9)على أنه (يجوز الإثبات في القضايا المصرفية بجميع طرق الإثبات بما في ذلك البيانات الإلكترونية أو البيانات الصادرة عن أجهزة الحاسب الآلي أو مراسلات أجهزة التلكس أو الفاكس أو غير ذلك= =

الجرائم المعلوماتية والتوصل إلى مقترفيها، إلا أنه يؤخذ على المشرع اليمني بهذا الشأن عدم إصدار تشريع موضوعي و إجرائي أو خاص يوضح تلك الجرائم والإجراءات التي يتعين اتخاذها بهدف الوقاية منها وكشفها في حال اقترافها، وصولا إلى معرفة الجاني أو الجناة ومعاقبتهم، فكيف يمكن الاعتماد على إثبات تلك الجرائم في ظل غياب النصوص القانونية التي تنظمها موضوعيا وإجرائيا، حيث أن المنطق يقتضي تضمين قواعد التجريم والمكافحة أولا ومن ثم فإن الإثبات سيكون تبعا لذلك، بحيث يمكن أعمال نصوص قانون المعاملات الإلكترونية، أو تضمين أو تعديل نصوص الإثبات وشموله على الاعتراف بالأدلة الرقمية في مجال الإثبات الجنائي لجرائم المعلوماتية.

وقد تميز القانون الجزائري عن اليمني بعدم الاكتفاء بالنصوص التقليدية التي تعطي سلطة تقديرية للقاضي في تقدير الدليل، حيث أعتمد على مبدأ حرية الإثبات كأصل، ونظام الأدلة القانونية كاستثناء[1]،وكذلك عدم الاكتفاء بالنصوص التي تعتد بأدلة الإثبات بالشكل الإلكتروني في المعاملات المدنية، وكذلك التوقيع الإلكتروني[2]، بل أن القانون الجزائري قد خول لسلطات المختصة الحق في تفتيش، وحجز، وتجميع الأدلة الإلكترونية عن طريق وضع ترتيبات تقنية تمكنهم من ذلك، إضافة إلى الاستعانة بكل

من الأجهزة المشابهة. كما يجب على البنوك والمؤسسات المصرفية الأخرى أن تحتفظ بالأوراق المتصلة بأعمالها لمدة لا تقل عن (10) سنوات بصورة مصغرة(ميكرو فيلم أو اسطوانة ممغنطة) أو غير ذلك من أجهزة التقنية الحديثة بدلا عن أصل الدفاتر والسجلات والوثائق والمراسلات والبرقيات والإشعارات وغيرها وتكون لهذه الصورة المصغرة حجية الأصل في الإثبات. وتعفى البنوك التي تستخدم في تنظيم عملياتها المالية والمصرفية الحاسب الآلي أو غيره من أجهزة التقنية الحديثة من تنظيم الدفاتر التجارية المنصوص عليها في القانون التجاري النافذ وتعتبر المعلومات المستقاة من تلك الأجهزة أو غيرها من الأساليب الحديثة بمثابة دفاتر تجارية لها حجية في الإثبات).

ونصت المادة (10) على: (يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس الآثار القانونية المترتبة على الوثائق والمستندات والتوقيعات الخطية من حيث إلزامها لأطرافها أو حجيتها في الإثبات).

وتعد ألمانيا وايطاليا أول دول تعتمد تشريع خاص بالإمضاء الالكتروني، الصادر في 13 جوان 1997مادة (3) فقرة (2)، والقانون الايطالي 15 مارس ،1997 المادة(15) راجع:

DIDIER Gobert et Étienne Montero: La signature dans les contrats et les paiements électroniques, cahiers du centre de recherches informatique et droit,Bruylant. Bruxelles. 2000,p.82.

(1) نصت المادة (212) من الأمر رقم (66- 155) المؤرخ في 8 يونيو1966 المتضمن قانون الإجراءات الجزائية، المُعَدَّل والمُتَمَّم على: (يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يبني حكمة بناء على اقتناعه الخاص، ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه).

(2) تضمنت المواد (323 مكرر، 323 مكرر1، 327) من القانون رقم (05- 10) المؤرخ في 20 يونيو 2005 المعدل والمتمم للقانون رقم (75 - 58) المؤرخ في 26 سبتمبر سنة 1975 المتضمن القانون المدني، على حجية الإثبات بالشكل الإلكتروني واعتبار التوقيع الإلكتروني حجة في الإثبات، حيث نصت المادة (323 مكرر) مدني ج على: (ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تضمنتها، وكذا طرق إرسالها). كما نصت المادة (323مكرر1) على أن: (يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها). كذلك فقد أعتدت الفقرة الأخيرة من المادة (327) بالتوقيع الإلكتروني بالشروط المذكورة في المادة السابقة. راجع: (ج.ر 44، ص24)

شخص مؤهل أو لدية علم بعمل النظام المعلوماتي المراد اتخاذ الإجراء بشأنه، وكذلك وضع عدد من الالتزامات على مقدمي الخدمات ومنها تقديم المساعدة للسلطات المختصة بالتحري أو التحقيق، بما من شأنه جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصال في حينها، وبوضع المعطيات المتعين عليهم حفظها تحت تصرف السلطات ومنها: المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، والخصائص التقنية، وكذا تاريخ ووقت ومدة كل اتصال، وكذلك المعطيات المتعلقة بالخدمة التكميلية المطلوبة أو المستعملة ومقدميها، والمعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها[1].

وطالما أن المشرع الجزائري قد سمح للسلطات المعنية بتجميع وحفظ الأدلة الإلكترونية والتعرف وتحيد هوية المرسل أو المرسل إليه وفقا لضوابط إجرائية، وألزم جهات أخرى بمساعدتها، فذلك وبدون أدنى شك أقرار صريح بحجية تلك الأدلة في الإثبات، بما فيها اعتماد برتوكول TCP/IP كدليل رقمي ذي حجية قضائية وذلك ما يجب على المشرع اليمني أن يقوم به.

وخلاصة ما سبق ومن خلال الإطلاع على مدى قبول حجية الدليل الإلكتروني في الإثبات الجنائي، يتضح بأن الإثبات الجنائي بالوسائل العلمية الحديثة، ومنها الوسائل الإلكترونية قد أضحى ضرورة في عصر تكنولوجيا المعلومات، هذا العصر الذي استخدمت فيه الحاسوبات الآلية، ونظم الشبكات لتبادل المعلومات والبيانات ومعالجتها، وغير ذلك من مجالات الحياة المختلفة، التي تسيرها أجهزة الحاسوب، ونظم الشبكات والبرامج والبيانات، فمن المعروف أن الجريمة ذات كيان معنوي ودليلها من ذات النوع، ومن ثم فإن حجية ذلك الدليل لابد أن تلاقي قبولا بها لدى جهات العدالة الجنائية، وفقا للشروط التي تخضع لها سائر الأدلة، ومن تلك الشروط عدم الحصول على الدليل بالإكراه، أو بأي طريقة غير مشروعة، كأن يتم التفتيش بدون إذن جهة التحقيق، في حالة أن يتطلب القانون ذلك، وغير ذلك من الشروطلتي يتطلبها القانون ما لم تراعِ أمور معينة تتناسب مع الدليل المعلوماتي، بشرط أن ينص القانون على ذلك. وبالرغم

([1]) راجع المواد (من 3-11) من القانون رقم (09-04)المؤرخ في 5 غشت(أغسطس)2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

من الخلاف حول حجية الدليل الإلكتروني في الإثبات فإن اتجاها دولياً قد ذهب نحو الاعتراف بالمراسلات الإلكترونية بمختلف أنواعها، والاعتراف بحجية الملفات المخزنة بالنظم ومستخرجات الحاسوب، وحجية الملفات ذات المدلول التقني البحت، وكذا حجية التوقيع الإلكتروني، والتخلي شيئا فشيئا عن أية قيود تحد من الإثبات في البيئة التقنية([1]).

وقد ذهب الفقه الفرنسي في مجال الإثبات بالأدلة الإلكترونية، انطلاقا من أن الأساس عندهم في الإثبات في الجانب الجنائي هو حرية الأدلة وحرية القاضي في تقدير هذه الأدلة، وتوسع أكثر في مسألة الإثبات بالأدلة الالكترونية عنها في مسألة قبول الأدلة العلمية[(2)].

وإذا كان البعض يشترط للإثبات تطلب مستندات ورقية، لكون المستندات الإلكترونية قابلة للتلاعب فيها بالحذف أو الإضافة أو التعديل، فإن تلك المشكلة قد تم التغلب عليها في ظل التطور التكنولوجي عن طريق استخدام برامج حاسب آلي تعمل على تحويل النص الذي يمكن التعديل فيه إلى صورة ثابتة، لا يمكن التدخل فيها أو تعديلها ويعرف هذا النظام باسم (Document image processing) ،كذلك فقد أمكن حفظ المحررات الإلكترونية في صيغتها النهائية وبشكل لا يقبل التبديل من خلال حفظها في صناديق الكترونية لا يمكن فتحها إلا بمفتاح خاص يهيمن عليه جهات معتمدة من قبل الدولة، بحيث تؤدي محاولة أطراف التعامل تعديل الوثيقة الإلكترونية إلى إتلافها أو محوها تماما[(3)].

وإذا كان هذا الرأي يبدو مقبولا في ضرورة التعامل مع الأدلة الرقمية، فإنه قد لا يبدو كذلك فيما يخص المبررات التي تم إبداؤها كمبررات لعدم تطابق ما قيل - من أن

([1]) يونس عرب، حجية الإثبات بالمستخرجات الإلكترونية في الأعمال المصرفية، مقال منشور في منتدى جامعة المنصورة، س .د 6 BM ت.د 2008/4/9 على الرابط:
http://www.f-law.net/law/showthread.php?p=156142

([2]) وتطبيقا لذلك فقد قضت محكمة النقض الفرنسية أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات تصلح لتقديمها أمام القضاء الجنائي راجع: مروك نصر الدين، مرجع سابق، ص468.

(3) عاصم عبد الجبار سعـــد،الإثبات في قانون المعاملات الإلكترونية العماني رقم(69)لسنة 2008،و قانون الإثبات في المعاملات المدنية والتجارية العماني رقم (86) لعام 2008 ، س .د 6 BM ت.د 2008/4/9 على الرابط:
http://www.ita.gov.om/ITAPortal_AR/Data/ImgGallery/FID200812383916827/%D8%A7%D9%84%D8%A5%D8%AB%D8%A8%D8%A7%D8%AA%20%D9%81%D9%8A%20%D8%A7%D9%84%D8%B9%D9%82%D8%AF%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%20%D8%AA%D8%B9%D8%AF%D9%8A%D9%84%20.doc

بالإمكان حفظ البيانات ومنع التلاعب بها، من خلال وسائل وبرامج حماية أمنية أو التشفير أو خلافه- مع واقع التكنولوجيا الرقمية وما يقوم به الهاكرز (hackers) أوالكراكرز(Crackers) من اختراقات للشفرات(Codes) والمفاتيح (keys) الخاصة بمواقع الأفراد والمؤسسات والشركات، ومن ثم قيامهم بالتلاعب بالبيانات المخزنة بتلك النظم، فالحماية الأمنية مثلما هي حماية رقمية، فإن الاختراقات التي تتم تستخدم فيها برامج قد تكون متطورة عن أنظمة الحماية، كما أن المجرم المعلوماتي التقني قد يمتلك من الخبرة مالا يملكه الخبراء والمختصون في مجال الأنظمة الأمنية، وبالتالي فإنه لا يمكن الاعتراف بأن تلك الأدلة لا تصلح أدلة إثبات، كما لا يمكن الأخذ بها على إطلاقها، بل لابد أن تتدخل الخبرة التي من المفترض أن يكون أصحاب الاختصاص ذوي إلمام كبير بها.

ولما تم ذكره، فإنه قد أصبح لزاما على التشريعات المختلفة مواكبة التطور الحادث في مجال التكنولوجيا الرقمية من خلال النص على إجراءات تتناسب والتعامل مع تلك الأدلة، وإعطاء القاضي صلاحيات تقديرية للتعامل مع تلك الأدلة.

فالرسالة الإلكترونية على سبيل المثال لا تتمتع بالثقة فيما يتعلق بهوية مرسلها ومدي إمكانية نسبة الرسالة إليه، وسلامة محتواها، وبالتالي فإن قوتها في الإثبات ستخضع لسلطة القاضي التقديرية، ومدى إلمامه وتفهمه بالنواحي التقنية الخاصة بتكنولوجيا المعلومات [1].

وبالتالي فإن الإثبات في القضايا الجنائية عن طريق الرسائل الإلكترونية يمكن قبوله بشرط التحقق من هوية المرسل ومكان الإرسال عن طريق(IP address).

وإذا كان الإثبات في بعض الحالات بالنسبة للمعاملات المدنية يتطلب في رسالة البريد الإلكتروني حتى تكون حجة أن تكون مذيلة بالتوقيع الإلكتروني، ذلك أن التوقيع الالكتروني يحدد الشيء الذي تم التوقيع عليه بشكل لا يحتمل التغيير، كما أنه أي التوقيع

([1]) موساي معمر،الإثبات الإلكتروني في القانون، منتدى الجزائرية للقانون والحقوق ،س.د am12 ،ت.د الأربعاء 2009/4/9.على الرابط:

http://forum.law-dz.com/index.php?showtopic=2661

وبهذا الشأن فيوجد قضية منظورة في المحكمة الجزائية المتخصصة في اليمن ، مفادها استخدام رسائل البريد الالكتروني في مجال التجسس لصالح إسرائيل، ونظرا للصعوبات الفنية والتقنية المتعلقة بكشف مثل هذه الجرائم فقد تم استدعاء خبيرين من وزارة المواصلات وتقنية المعلومات، للاستعانة بهم، وما زالت قيد إجراءات المحاكمة في الاستئناف.

الرقمي يقوم على وسائل التشفير بما تتضمن من اعتماد على معادلات حسابية، ولا يُكتفَ بذلك فحسب، بل أنه توجد جهة وسيطة تصادق على التوقيع الرقمي بحيث تكشف وتمنع التلاعب به، فإذا كان الإثبات في بعض المعاملات المدنية يتطلب مثل تلك الشروط، فإن الإثبات في الجانب الجنائي من باب أولى يجب أن يراعى فيه التحري، والدقة، والشروط الموضوعية التي تراعي من خلالها الموازنة بين حرية الأفراد في المحافظة على خصوصياتهم، وحق المجتمع في أمنه واستقراره بإنزال العقاب على المجرمين.

إضافة إلى ما سبق فإنه يجب توافر عدد من الشروط في المخرجات الكمبيوترية حتى يمكن قبولها كأدلة في الإثبات الجنائي أهمها:

1- مبدأ يقينية المخرجات الكمبيوترية

يقوم هذا المبدأ على ضرورة أن يتيقن القاضي من يقينية المخرجات الكمبيوترية، واليقين في النظم الإجرائية هو :حالة ذهنية أو عقلانية تؤكد وجود الحقيقة عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي، من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات ثقة عالية من التوكيد[1].

فالمحقق أو القاضي الذي يعاين جسم الجريمة عن طريق حواسه، لا يمكنه معاينة الفعل الجنائي لحظة وقوعه، وإنما يستطيع معاينة النتائج التي ترتبت عليه، وعن طريق التحليل والاستنتاج يمكن التوصل إلى الكيفية التي تمت بها الجريمة، والأداة التي استخدمت فيها، والآثار التي تدل على شخصية مرتكبها .

واليقين ذو خاصية شخصية، أو نفسية تختلف من قاضي إلى أخر، ومن ثم فإن القناعة التي يمكن أن يتوصل إليها قاض في قضية معينة، لا يتوصل إليها قاضٍ في قضية مماثلة، ويترتب على ذلك احتمال حدوث أخطاء أثناء ممارسة هذا المبدأ، ولذلك يجب أن يتسم هذا المبدأ بالثبات، أو ما يمكن تسميته باليقين الثابت، وهو اليقين المشترك بين جميع القضاة بخصوص إدانة أو براءة شخص معين ([2]).

([1]) علي محمود حمود:مرجع سابق منشور على شبكة المعلومات الدولية على الرابط:
Http://www.f-law.net/law/shozthread.php?t=1133

(2) هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، مرجع سابق، ص81.

وإذا كانت هذه الأحكام التي تحكم اليقين في الأدلة الجنائية، فإن الأمر لا يختلف بالنسبة لمخرجات الحاسب الآلي، حيث يجب أن يشترط في المخرجات الكمبيوترية أن تكون يقينية، حتى يمكن الحكم بالإدانة على ضوئها، ذلك أن لا محل لدحض قرينة البراءة وإثبات عكسها، إلا عندما يصل اقتناع القاضي إلى درجة الحزم واليقين، ويتم ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي، من خلال ما يعرض عليه من مخرجات كمبيوترية، سواءً أكانت مخرجات ورقية تنتجها الطابعة(printers)، أو الراسم(ploter)، أم كانت مخرجات الكترونية كالمصغرات الفيلمية (Computer output microfilm) والأشرطة المغناطيسية(Magnetic Tape)، أو الأقراص المغناطيسية (Magnetic disks) أم غيرها من الأشكال غير التقليدية للتكنولوجيا التي تتوافر عن طريق الوصول المباشر، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الكمبيوتر على الشاشة الخاصة به، أو على إحدى الطرفيات.

2- مناقشة مخرجات الوسائل الإلكترونية

يعد مبدأ مناقشة المخرجات الكمبيوترية من المبادئ التي تساعد في حل المشكلات المتعلقة بحجية المستخرجات الكمبيوترية في الإثبات الجنائي، ذلك أن مناقشة تلك الأدلة من قبل القاضي أمام الخصوم، سواء أكانت مخرجات ورقية بشكل أوراق مطبوعة، أم وسائط الكترونية، حيث يكون باستطاعة القاضي أن يبني قناعته بتلك الأدلة لا بعلمه أو بعلم غيره، لأن القناعة التي تولدت لديه هي جزء من مناقشة تلك الأدلة التي عن طريقها تتضح قوة الأدلة من ضعفها، وبالتالي فستبنى لدى القاضي قناعة بتلك الأدلة أو بتركها.

3- مشروعية الأدلة المتحصلة من الوسائل الإلكترونية

حتى يكون للأدلة الإلكترونية حجية في الإثبات الجنائي، يجب أن يكون الحصول على تلك الأدلة قد تم بطرق مشروعة، وبالتالي فإن استخدام الوسائل غير المشروعة للحصول على الأدلة الإلكترونية يترتب عليها بطلان الإجراء، كأن يتم الحصول على كلمة السر أو الشفرة الخاصة بالدخول إلى النظام عن طريق الإكراه أو التعذيب، سواءً كان مادياً ام معنوياً ، وكذلك استخدام التدليس أو الغش في الوصول إلى الأدلة

الإلكترونية، وغير ذلك من الأساليب المخالفة للقوانين وتتضمن اعتداءات على الضمانات والمبادئ المتعلقة بحقوق الإنسان وخصوصياته [1].

فالأدلة الإلكترونية بالرغم من كونها أدلة غير مادية، إلا أنها إذا ما طبقت عليها الشروط سالفة الذكر فلا يوجد ما يمنع من الأخذ بحجيتها في الإثبات، استنادا إلى مبدأ قناعة القاضي في الأخذ بالدليل الإلكتروني بعد التوصل إلى تلك القناعة بيقين ذلك الدليل، وبعد مناقشته بحضور الخصوم، وبشرط أن تكون وسائل الحصول عليه مشروعة، فكل ذلك يؤكد بأنه لم يعد ما يبرر بعدم الأخذ بالدليل الالكتروني، لأن أدنى شبة لدى القاضي في يقينية الدليل، أو عدم مشروعيته تجعل القاضي لا يعتبره حجة للإدانة في القضية المنظورة لديه.

---

(1) راجع هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص11ص وما بعدها.

المبحث الثاني

التـــعــــاون الدولــــي

لقد أضحت مكافحة وملاحقة الجرائم المعلوماتية امرأ في غاية الأهمية بسبب المخاطر الجمة الناتجة عنها والتي تفوق بكثير المخاطر الناتجة عن الجرائم التقليدية، حيث لم تقتصر تلك المخاطر على إقليم بذاته أو دولة بعينها، بل إن مخاطرها قد شملت أغلب الدول باختراقها للحدود الدولية، لأنها جريمة عابرة للحدود، وأكثر من ذلك أن تلك المخاطر قد ترتبط بأكثر من دولة في نفس الوقت، فقد يُرتكب السلوك الإجرامي في دولة وتتحقق النتيجة في أكثر من دولة.

ونتيجةً لتلك المخاطر، إضافة إلى المعوقات المتعلقة بهذه الجرائم وتتعلق بالجوانب الإجرائية التي سبق الإشارة إليها، وكذلك قصور التشريعات الوطنية في موجهة تلك الجرائم، فقد تم عقد العديد من الاتفاقيات الدولية بهدف مكافحة تلك الجرائم[1]، و أصبح لزاما وجود تعاون دولي لمكافحتها، إلا أَن ذلك التعاون لم يرقَ إلى المستوى المطلوب فيما بين الدول باستثناء عدد من الاتفاقيات الدولية التي تطرقت لإيجاد صيغة تعاونية دولية لمكافحة تلك الجرائم، ويأتي على رأسها اتفاقية بودابست حيث تمثل المرجع العام للعديد من التشريعات، لذلك سيتم التطرق إلي دور الاتفاقية في مواجهة الإشكاليات في الجوانب الإجرائية لجرائم المعلوماتية، إضافة إلى أهمية التعاون الدولي للحد من تلك المشكلات، حيث سيتم التعرض للاتفاقية في موضع أول وفي الموضع الثاني سيتم إيضاح ضرورة التعاون الدولي في مجال مكافحة الإجرام المعلوماتي.

(1) لعبت الاتفاقيات الدولية دورا مهما في معالجة المشكلات الناتجة عن الجرائم المعلوماتية سواءً في الجانب الموضوعي أم الإجرائي، حيث تطرقت في الجانب الموضوعي إلى أهم أنوع الجرائم التي يجب النص عليها في القوانين الداخلية للدول، أما في الجانب الإجرائي فقد تطرقت إلى أهم الإجراءات المتعلقة بكشف وضبط جرائم المعلوماتية ومرتكبيها وتتناسب مع تلك الجرائم وأدلتها، والتي يجب النص عليها في القوانين. وأهم تلك الاتفاقيات اتفاقية بودابست، حيث تعد الاتفاقية الأهم في مجال محاربة الإجرام المعلوماتي، نظرا للعدد الهائل من الدول التي وقعت عليها، وباعتبارها الاتفاقية الأشمل في مجال مكافحة جرائم التكنولوجيا الحديثة، كما توجد العديد من الاتفاقيات في ذات المجال ومنها اتفاقية الأمم المتحدة وتوصيات مجلس أوربا لعامي 1989، و1995.

المطلب الأول

الإجراءات المستحدثة وضمانات المتهم

تعد اتفاقية بودابست من أهم الاتفاقيات التي تطرقت إلى ضرورة اتخاذ التدابير التشريعية والتنظيمية لمتابعة وكشف جرائم المعلوماتية، وتوفير قواعد ملائمة للتحري، والتحقيق، والمحاكمة، و التركيز على أهمية التعاون الدولي [1].

([1]) أبرمت اتفاقية بودابست بتاريخ 23 /2001/11 حول مكافحة الإجرام ألمعلوماتي في مدينة بودابست عاصمة دولة المجر ضمت 26 دولة من أعضاء الاتحاد الأوربي، إضافة إلى أربع دول من خارج الاتحاد وهي الولايات المتحدة الأمريكية واليابان وكندا وجنوب أفريقيا، وتعد أول اتفاقية دولية تسعى لوضع الحماية الجنائية الموضوعية والإجرائية للجرائم المعلوماتية وإقرار التعاون الدولي بشأن مكافحتها، إيمانا من الدول الأعضاء في مجلس أوروبا والدول الأخرى التي وقعت على الاتفاقية بالتغيرات التي حدثت بسبب الرقمية، ولقد مرت الاتفاقية بعدد من المراحل قبل إقرارها بالصيغة النهائية، فلقد بدأت فكرة لاتفاقية في مجال مكافحة الإجرام المعلوماتي عام 1989 بقيام مجلس أوربا بإصدار توصيات تتضمن ضرورة تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسوب ومن تلك التوصيات التوصية رقم (Recommandation No. 89- 9)، كما تبعتها دراسة تبناها مجلس أوربا في عام 1995تضمنت العديد من التوصيات منها التوصية رقم (Recommandation No. 95- 13) حول الإجراءات الجنائية في مجال جرائم الانترنت، وعلى أساس المبادئ التي تضمنتها هاتان التوصيتان فقد قام مجلس أوربا عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي بقصد إعداد اتفاقية تضمن تسهيل التعاون الدولي في الإجراءات الجنائية في الجرائم الناشئة عن استخدام الحاسوب والإنترنت، وفي ابريل من العام 2000 صدر أول مشروع لهذه الاتفاقية بعنوان"اتفاقية الجريمة عبر العالم الافتراضي"وفي 19 /2001/9، أي بعد إعداد المشروع، فقد تمت الموافقة عليه من قبل سفراء الدول الأوربية الـ 43 في المجلس تمهيدا لعرضها على وزراء الخارجية في اجتماعهم المنعقد في ستراسبورج في نوفمبر 2001 وتمت الموافقة عليه من قبلهم في هذا التاريخ، وفي 23 /2001/11 تم التوقيع النهائي على الاتفاقية، وتضمنت الاتفاقية (48) مادة موزعة في أربعة فصول، حيث تضمن الفصل الأول المصطلحات الأساسية من خلال(المادة 1)، بينما تضمن الفصل الثاني ثلاثة أقسام : القسم الأول: يضم المواد من 2 – 13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر، والقسم الثاني: يضم المواد من 14 – 21 وتتعلق بالقواعد الإجرائية، والقسم الثالث: يضم المادة 22 وتعلق بالاختصاص . أما الفصل الثالث من الاتفاقية فقد جاء تحت عنوان التعاون الدولي وتضمن قسمين، الأول: تحت عنوان المبادئ العامة ويضم المواد من 23-28 والقسم الثاني: يتعلق بالنصوص الخاصة ويضم المواد من 29-35 . أما الفصل الخامس والأخير فيتضمن الأحكام الختامية ويضم المواد من 36 – 48 . راجع: هلالي عبد اللاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص159 وما بعدها. وعمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص199 وما بعدها .وكذلك جريدة الشرق الوسط، السبت 08 رمضان 1422 هـ 24 نوفمبر 2001 العدد **8397**،على الربط:

http://www.aawsat.com/details.asp?section=1&article=67899&issueno=8397

وراجع سعود بن عبد العزيز المريشد، غسل الأموال الإلكتروني وفقا للنظام السعودي والنظام المقارن والمعايير الدولية، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني، الذي تم تنظيمه من قبل رأسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر 2007، مجلد 1 ص 524.

يونس عرب: تطور التشريعات في مجال مكافحة الجرائم المعلوماتية، ورقة عمل قدمت إلى ورشة العمل التي تبنتها هيئة تنظيم الاتصالات بسلطنة عمان،2-4 ابريل 2006 ،منشوره على شبكة المعلومات الدولية على الربط:

http://www.ituarabic.org/coe/2006/E-Crime/Documents%20and%20Presentations/DAY%201/Doc6-Jor.DOC

ولرجوع إلى نصوص الاتفاقية باللغة الفرنسية انظر شبكة الانترنت على الرابط:

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

وراجع ايضا:

Guy De Vel, <<La convention sur la cybercriminalité>>, Le droit international de l'internet, Bruylant, Bruxelles,2002,p .238.

وقد تضمنت الاتفاقية عدد من النصوص المتعلقة بمعالجة المشكلات الإجرائية في المواد (14-22) ومن تلك المشكلات التي تطرقت لها الاتفاقية :

1- الضمانات الشرعية

تضمنت المادة (14)أحكام عامة تتعلق بمعالجة مشكلة عدم تضمين بعض القوانين نصوص إجرائية خاصة بمكافحة هذه الجرائم، وكذا إنشاء السلطات المعنية بالتنقيب والإجراءات الجنائية، تحت مسمى نطاق تطبيق قانون الإجراءات الجنائية، إذ يبدو جليا أن أغلب التشريعات مازالت تفتقر إلى النصوص القانونية الإجرائية الخاصة بالتنقيب أو التحري أو التحقيق، وتعمل بالقواعد التقليدية التي أصبحت إن لم تفِ فهي لا تكفي لملاحقة ومتابعة وكشف الجرائم ذات البعد الرقمي[1].

وقد تضمنت المادة سالفة الذكر إلزام كل دولة طرف في الاتفاقية بتبني الإجراءات التشريعية، أو أي إجراءات أخرى ترى أنها ضرورية وفقا لقانونها الداخلي والأطر القانونية، من اجل إنشاء وتأسيس سلطات وإجراءات مما نصت عليها الاتفاقية بغرض التنقيبات والإجراءات الجنائية النوعية [2].

---

(1) Guy De Vel, Op. Cit, p.242.

(2) أنظر المادة (14) من اتفاقية بودابست لمكافحة الإجرام المعلوماتي ،2001. وقد ورد نص المادة بالفرنسي :

Article 14 – Portée d'application des mesures du droit de procédure

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.
2- Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:
a- aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;
b- à toutes les autres infractions pénales commises au moyen d'un système informatique; et
c- à la collecte des preuves électroniques de toute infraction pénale.
3- a-Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.
b- Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:=

وتشير ذات المادة إلى أن الإجراءات والسلطات التي تم تأسيسها وفقا لما تضمنته نصوص الاتفاقية تنطبق على الجرائم المعلوماتية المنصوص عليها في القسم الأول من الاتفاقية والتي تم إيضاح عدد منها أثناء تناول الجرائم المعلوماتية المستحدثة - ومنها جريمة الدخول والبقاء عن طريق الغش إلى نظام المعالجة الآلية للمعطيات-

وغيرها من الجرائم التي تضمنتها الاتفاقية [1].وكذلك فإن السلطات والإجراءات التي يتم تأسيسها تنطبق على كل جريمة أخرى ترتكب بواسطة نظام معلوماتي، وعلى جميع الأدلة الالكترونية لكل جريمة جنائية، ويستثنى من الإجراءات المشار إليها حالتين:

الأولى: نصت عليها المادة(21) من الاتفاقية وذلك بجعل اعتراض البيانات المتعلقة بالمحتوى مقتصراً على الجرائم الخطيرة التي تضمنتها القوانين الداخلية للدول الأعضاء، مراعاة لطابع السرية.

والثانية: تكمن في أن أي طرف له الحق أن يتحفظ في عدم تطبيق الإجراءات المشار إليها في المادة (20) من الاتفاقية (الجمع في وقت فعلي لبيانات المرور) إلا على الجرائم أو طوائف الجرائم المحددة في التحفظ بشرط أن لا يكون نطاق أو طوائف هذه الجرائم أكثر تقييدا من نطاق الجرائم التي تنطبق عليها إجراءات الاعتراض المشار إليها في المادة(21) الخاصة باعتراض البيانات المتعلقة بالمحتوى.

=i qui est mis en œuvre pour le bénéfice d’un groupe d’utilisateurs fermé, et
ii qui n’emploie pas les réseaux publics de télécommunication et qui n’est pas connecté à un autre système informatique, qu’il soit public ou privé,
cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l’application la plus large possible de la mesure mentionnée aux articles 20 et 21.

انظر شبكة المعلومات الدولية http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

(1) والجرائم التي تضمنتها الاتفاقية ونصت بأنه يجب على الدول الأطراف في الاتفاقية النص عليها في تشريعاتها منها جرائم تستهدف عناصر امن المعلومات وتشمل جريمة الدخول غير القانوني (مادة 2) والاعتراض غير القانوني (مادة 3) والتدخل في المعطيات (مادة 4) والتدخل في نظم الحاسوب (مادة 5) وإساءة استخدام الأجهزة (مادة 6)، ومنها الجرائم المرتبطة بالكمبيوتر، وتشمل التزوير المرتبط بالكمبيوتر (مادة 7) والاحتيال المرتبط بالكمبيوتر (مادة 8)، ومنها جرائم المحتوى، وهي جرائم دعارة الأطفال (المادة 9)، ومنها جرائم مرتبطة بحق المؤلف والحقوق المجاورة وتشمل الجرائم الجنائية التي تعد اعتداءا على المصنفات المحمية بحق المؤلف والحقوق المجاورة (مادة 10) ،ومنها جرائم الشروع attempt والمساعدة aiding والتحريض abetting (مادة 11) ومسؤولية الأشخاص المعنوية corporate liability (مادة 12) ومعايير العقاب sanctions and measures (مادة 13).

وعموما فإن الاتفاقية تدعو الأطراف التي تمارس حق التحفظ إلى تحديد تحفظها بطريقة تسمح بتطبيق سلطات وإجراءات أوسع من أجل جمع البيانات المتعلقة بالمرور في وقت فعلي .

كما تقرر الاتفاقية في الفقرة (ب) من المادة(14) على إمكانية التحفظ للدول بسبب وجود قيود في قوانينها الداخلية، في وقت تبني الاتفاقية، بحيث لا يمكنها اعتراض الاتصالات التالية:

- الاتصالات عبر النظم المعلوماتية التي تعمل لصالح مجموعة مغلقة من المستخدمين، تقتصر على تقديم خدمة معينة.
- الاتصالات التي لا تستخدم شبكة عامة للاتصال عن بعد بما في ذلك الإنترنت، أو شبكات التلفونات العامة، أو أي من طرق الاتصال عن بعد، يتم من خلالها انتقال الاتصالات.
- الاتصالات التي لا تتصل بنظم معلوماتية أخرى سواءً أكانت الصلة بين هذا النظام وذاك ماديةً أم معنوية .

وبهذا فإن الاتفاقية قد عالجت من خلال نص هذه المادة القصور التشريعي إزاء مواجهة جرائم المعلوماتية، بحيث ألزمت الدول الأطراف في الاتفاقية بالنص على الجرائم المعلوماتية التي تضمنتها الاتفاقية، وكذا الإجراءات والسلطات الخاصة بالتنقيب[1]، وكافة الإجراءات النوعية التي يمكن اتخاذها بصدد كشف تلك الجرائم ومتابعة الجناة ومعرفتهم، بحيث تمثل تلك الإجراءات والتوصيات الحد الأدنى التي يجب على الدول الأعضاء في الاتفاقية النص عليها في قوانينها.

([1]) التنقيب في قواعد البيانات من الأمور الجوهرية التي توصل إلى كشف الجريمة، وهذا التنقيب له خطواته التي يجب على سلطات التنقيب إتباعها ومنها: تحديد المشكلة المراد بحثها، وبناء قاعدة بيانات، واستكشاف البيانات، وتحضير البيانات للتنقيب، وبناء نموذج التنقيب المناسب، وتطبيقه، واستخراج النتائج. ولذلك فقد أصبح علم التنقيب والتحليل في قواعد البيانات من الهموم الكبيرة التي تقع على عاتق الدول بشتى مؤسساتها. راجع : مصطفى فواد عبيد، التنقيب في قواعد البيانات واستكشاف المعلومات المخبأة فيها، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني،الذي تم تنظيمه من قبل رأسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر 2007، مجلد 2، ص1277.

ومع أن بعض الدول قد سبقت تلك الاتفاقية في إصدار قوانين أو نصوص قانونية تضمنت تجريم ذلك النوع المستحدث من الإجرام وكيفية مواجهتها[1]، إلا أن تلك الاتفاقية قد وحدت جهود الدول الموقعة عليها في مجال التعاون الدولي لمكافحتها وتعديل النصوص القانونية بما يتواكب مع نصوص تلك الاتفاقية .

كما أن الاتفاقية قد تضمنت المعالجة إلى حد ما للمشكلة التي مفادها أن الإجراءات المتعلقة في مجال الجرائم المعلوماتية تتسبب في الاعتداء على حقوق وحريات الأشخاص ودقائق خصوصياتهم، بما تتضمنه من إطلاع وتفتيش أغلب إن لم يكن جل بيانات ومعلومات الأشخاص المخزنة في أنظمتهم، والتي لم يكن الإطلاع عليها ومعرفة خباياها بهذه السرعة لولا تلك التكنولوجيا، بما تتميز به من قدرات لتخزين الكم الهائل من المعلومات، وكذلك الإطلاع عليها وكشف خباياها، حتى أن الإنسان قد أضحى مكشوفا في أموره العامة والخاصة.

وقد عالجت الاتفاقية ذلك في كونها ربطت الإجراءات والسلطات باحترام ومراعاة حقوق الإنسان وخصوصياته، بما ينسجم مع الاتفاقيات والمواثيق الدولية المتعلقة بحماية حقوق الإنسان وحرياته الأساسية، وأن على الدول تضمين ذلك في دساتيرها وقوانينها.

وبناء على ما سبق فإن الإجراءات والسلطات التي تلزم بها الاتفاقية الأطراف بتضمينها في قوانينها، يجب أن تخضع للشروط والضمانات التي يقررها القانون الداخلي للدولة العضو، والذي بدوره يجب أن يضمن حماية كافية لحقوق الإنسان وحرياته، ومنها الالتزامات التي تضمنتها اتفاقية المجلس الأوربي لحماية لحقوق الإنسان وحرياته الأساسية لعام 1950، والاتفاقية الدولية للحقوق المدنية والسياسية للأمم المتحدة لعام 1966.

وكذلك الاتفاقيات العالمية الأخرى لحماية حقوق الإنسان وحرياته الأساسية.

وهذه الشروط والضمانات يجب أن تتكامل مع مبدأ التناسب، مع طبيعة وظروف الجريمة، بحيث يشترط أن تقوم بتلك الإجراءات، أو تشرف عليها جهات قضائية أو

(1) ومن تلك الدول التي ضمنت قوانينها تجريم المساس بأنظمة المعالجة الآلية للبيانات أو المعلومات المدرجة بها أو المنقولة من نظام إلى آخر عبر الشبكات سواءً كانت محلية أم دوليه فرنسا، وبلجيكا، والولايات المتحدة الأمريكية، وبريطانيا.

جهة أخرى مستقلة، أو أن ترتبط تلك الشروط والضمانات بالبواعث المبررة لتطبيق السلطة أو الإجراء،وكذلك تحديد تبعته ومدته [1].

وإذا كانت الدول الأعضاء ملزمة بإدخال بعض الضوابط لتقويم الإجراءات الجنائية في قوانينها الداخلية، إلا أن نماذج التبني وتنفيذ هذه السلطات والإجراءات متروك للنظام الإجرائي لكل دولة على حدة.

وبهذا الخصوص فإن الجزائر وإن لم تكن من الدول الموقعة على الاتفاقية، إلا أنها تعمل جاهدة على متابعة التشريعات والاتفاقيات ذات العلاقة بجرائم التكنولوجيا وتقوم بوضع التشريعات التي تعني بمواجهة تلك الجرائم موضوعيا وإجرائيا، بغض النظر عن القصور التي قد ترافقها كغيرها من التشريعات بسب التطور السريع لتلك الجرائم وأسلوب ارتكابها.

وفي الجانب الإجرائي الذي نحن بصدد دراسة المشاكل التي ترتبط به فقد قام المشرع الجزائري بإصدار قانون في نهاية 2009 للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتضمينه الإجراءات التي تتناسب ومكافحة تلك الجرائم ذات الطابع التقني، وتحديد السلطات المناط بها اتخاذ تلك الإجراءات[2].

([1])راجع المادة (15) من اتفاقية بودابست 2001. و نص المادة بالفرنسي:

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l’instauration, la mise en œuvre et l’application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l’Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d’autres instruments internationaux applicables concernant les droits de l’homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d’autres formes de supervision indépendante, des motifs justifiant l’application ainsi que la limitation du champ d’application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l’intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l’effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

([2]) اصدر المشرع الجزائري القانون رقم(09- 04) المؤرخ في 5 غشت(أغسطس)2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تضمن في الفصل الأول الهدف منه، ومعانى بعض المصطلحات ذات الطابع التقني ومجال التطبيق، وفي الفصل الثاني وضح الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، وفي الفصل الثالث تم بيان القواعد الإجرائية المتعلقة بتفتيش نظم المعلوماتية=

2- التوصيات الدولية في الإثبات بالدليل الإلكتروني

ومن تلك التوصيات فقد تضمنت اتفاقية بودابست بعض الإجراءات القانونية الجديدة لمواجهة بعض المشكلات المتعلقة بالدليل الالكتروني والمتمثلة بتبخر المعلومات، التي يمكن أن تعد أدلة يستفاد منها في معرفة الحقيقة والوصول إلى الجاني، وكذلك سهولة أخفاء الدليل في حالة معرفة الجاني بأنه سوف يتم تعقبه والتفتيش على تلك المعلومات التي تدينه، ومن تلك الإجراءات الجديدة التي تضمنتها الاتفاقية:

أ- التحفظ العاجل على البيانات

تطرقت الاتفاقية لإجراء التحفظ على البيانات المخزنة في نظام معلوماتي، بما فيها بيانات المرور[1]، حيث ألزمت الدول الموقعة على الاتفاقية باتخاذ الإجراءات التي ترى أنها ضرورية من أجل السماح للسلطات المختصة في أن تأمر بالتحفظ العاجل على البيانات المعلوماتية المخزنة، بما فيها البيانات المتعلقة بالمرور، والمخزنة بواسطة نظام معلوماتي، وعلى وجه الخصوص عندما تكون هناك أسباب تدعو للاعتقاد بتعرض تلك البيانات للفقدان أو التلف، ويكون ذلك عن طريق أمر توجهه السلطة لحائز البيانات شخصا كان أم شركة، لإجبار هذا الشخص أو تلك الشركة على التحفظ على البيانات فترة من الزمن قدرتها الاتفاقية ب90 يوما كحد أقصى قابلة للتجديد في حال أن رأت السلطة ذلك.

ويجب كذلك على كل طرف اتخاذ الإجراءات التشريعية أو أي إجراءات ضرورية لإجبار حائز البيانات، أو أي شخص يقع عليه عبئ التحفظ على البيانات، أن يحافظ على

= وحجز المعطيات، وفي الفصل الرابع تم الإشارة إلى التزامات مقدمي الخدمات لمساعدة السلطات في حفظ البيانات المتعلقة بحركة السير، وفي الفصل الخامس تم بيان المهام الخاصة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم إنشائها بموجب هذا القانون، وتضمن الفصل السادس والأخير التعاون والمساعدة القضائية الدولية بداية بالاختصاص القضائي، والمساعدة الدولية القضائية، وتبادل المعلومات واتخاذ الإجراءات التحفظية، والقيود الواردة على طلبات المساعدة القضائية الدولية، وقد تم إيضاح العديد من نصوص هذا القانون أثناء تناول المشكلات المتعلقة بالاستدلال والتحقيق.

([1]) تعرف بيانات المرور(traffic data) بأنها :"كل البيانات التي تتعامل مع الاتصال، والتي تمر من خلال النظام المعلوماتي، أو يتم إعدادها بواسطته، والذي يعد عنصرا في سلسلة الاتصال، بالإشارة إلى مصدر الاتصال، ومكان الوصول، وخط السير، والسرعة، والتاريخ، والحجم، ومدة الاتصال، ونوع الخدمة ألمؤداه" وقد وردت في القانون الجزائري رقم (09-04) 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تحت مسمى المعطيات المتعلقة بحركة السير.راجع: المادة(1) من اتفاقية بودابست بشأن مكافحة الإجرام المعلوماتي،2001، والفقرة (هـ) من المادة (2) من القانون الجزائري المشار إليه.

ولتفصيل أكثر حول الإجراءات المستحدثة والتي منها التحفظ العاجل على البيانات راجع:

Stéphanie Perrin: Cybercriminalité, article publié sur internet, date d'entrée 20/06/2009. http://www.vecam.org/article657.html

السرية بالنسبة لتطبيق الإجراءات التي تتم خلال المدة المقررة[1]، والهدف من الحفاظ على السرية لتجنب أن يقوم أشخاص آخرين بتغيير البيانات أو محوها، وبهدف الحفاظ على الحق في الخصوصية.

وقد تضمن القانون الجزائري الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في إطار تطبيقه، عدد من الالتزامات على مقدمي الخدمات ومنها: تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطة المذكورة مع مراعاة سرية العمليات والمعلومات المتصلة بها.

ولحفظ البيانات المتعلقة بحركة السير، يتعين على مقدمي الخدمات حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية

---

(1) راجع المادة(16)من اتفاقية بودابست بشأن مكافحة الإجرام المعلوماتي. مشار إليها لدى هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق ،ص195، ص196. والنص بالفرنسي:

Article 16 – Conservation rapide de données informatiques stockées

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d’ordonner ou d’imposer d’une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.
2- Lorsqu’une Partie fait application du paragraphe 1 ci-dessus, au moyen d’une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d’obtenir leur divulgation. Une Partie peut prévoir qu’une telle injonction soit renouvelée par la suite.
3- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.
4- Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

شبكة المعلومات الدولية، مرجع سابق، على الربط: http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

المستعملة للاتصال، وكذلك حفظ الخصائص التقنية، وتاريخ ووقت ومدة كل اتصال، والمعطيات المتعلقة بالخدمة التكميلية المطلوبة أو المستعملة ومقدميها، والمعطيات التي تسمح بالتعرف على المرسل إليه، أو المرسل إليهم الاتصال، وعناوين المواقع المطلع عليها.

وبالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا تلك التي تسمح بالتعرف على مصدر الاتصالات وتحديد مكانها. وتحدد مدة حفظ المعطيات المذكورة بسنة واحدة ابتداء من تاريخ التسجيل.

وتقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي الإخلال بالتزامات المذكورة إلى عرقلة حسن سير التحريات القضائية، حيث يعاقب الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 د.ج إلى 500.000 د.ج، ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات[1].

ويعد التحفظ بالنسبة لغالبية الدول إجراءً قانونيا جديدا، فهو أداة جديدة للتنقيب والتحري في مجال مكافحة الإجرام المعلوماتي لعدة مبررات[2]:

- قابلية البيانات للتلاشي وبالتالي فقدان عناصر إثبات الجريمة، وبدلا من قيام السلطات بإجراء تفتيش - سواءً عن بعد أو بعد الانتقال إلى المكان الذي تقع فيه الأجهزة لتفتيشها، أو الولوج من قبل السلطة المختصة إلى النظام لضبط البيانات - وخاصة عند وجود الثقة لدى الشخص أو الجهة التي توجد لديها البيانات وبهدف السرعة حتى لا يتم التلاعب في البيانات أو محوها، فإن السلطة المختصة تقوم عوضا عن التفتيش، باستصدار أمر بالتحفظ على البيانات لدى الشخص، أو الجهة حائزي البيانات، أو المشرفين عليها، وبذلك فإن أمر التحفظ يكون اقل ضررا من عملية التفتيش، ويحقق نتائج ايجابية في المحافظة على البيانات من التلاعب بها، أو إخفائها، أما في حالة أن لا يكون الشخص أو الجهة حائزي البيانات جديرين بالثقة، فإن أجراء التفتيش والضبط يكون أجدى من إجراء التحفظ.

(1) راجع المادة (10) والمادة (11) من القانون رقم (09 - 04) المؤرخ في 5 غشت (أغسطس) 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
(2)هلالي عبد اللاه أحمد، مرجع سابق، ص190.

- الجرائم المعلوماتية غالبا ما يتم ارتكابها عن طريق نقل الاتصالات بواسطة نظام معلوماتي، وهذه الاتصالات يمكن أن يكون محتواها غير مشروع كمواد إباحية، أو فيروسات معلوماتية، أو أية تعليمات تحمل اعتداء على البيانات، أو تعيق أداء النظام المعلوماتي، كما يمكن أن تحوي عناصر يمكن من خلالها إثبات أن جرائم أخرى قد تم ارتكابها، مثل جريمة النصب، أو الاتجار بالمخدرات، أو الاعتداء على الخصوصية، أو الملكية الفكرية، وبناء على ذلك فإن التحقق من هوية مصدر الاتصالات، أو منتهاها يمكن أن يساعد على تحديد هوية مرتكب الجريمة.
- إن التحفظ على الاتصالات بواسطة مقدمي الخدمات، ومنها على سبيل المثال البريد الالكتروني، يكون هاماً جداً من اجل عدم فقدان عناصر الإثبات الجوهرية، فإعطاء صورة من البريد المخزن يمكن أن يكشف عن الجرائم التي تم ارتكابها.

ولكون إجراء التحفظ وقتي، فإن على السلطة القائمة عليه أن تحدد فترة التحفظ بفترة زمنية محددة، ولا يجب الكشف عن تلك البيانات للسلطة القسرية، ولابد من اتخاذ إجراء إضافي، أو أمر بالتفتيش بعد إجراء التحفظ للبحث عما يفيد في كشف الجريمة.

أما ما يخص العمل بالدليل الاليكتروني وحجيته في الإثبات، فقد أشارت الاتفاقية إلى أن الدول الأعضاء في الاتفاقية يجب أن تضمن قوانينها الداخلية النص على أن المعلومات سواءً اتخذت شكلا رقميا أم إلكترونياً، فإنها يمكن أن تستخدم في- كلتا الحالتين – كدليل الكتروني أمام القضاء، في إطار الإجراءات الجنائية التي تكون موضعا للمحاكمات الجنائية[1]، ومع ذلك فإن الدليل الالكتروني سوف يخضع للسلطة التقديرية للقاضي، على ضوء النظام الذي يوسع من تلك السلطة- اللاتيني- أو الذي يقيدها بالدليل القانوني - الانجلوسكسوني- وفقا لما تم التنويه إليه سابقا.

ب- التحفظ والإفشاء العاجلان لبيانات المرور

وهذا الإجراء أيضا يعد من الإجراءات الجديدة التي أتت به اتفاقية بودابست، بهدف نجاح التنقيب والتحري في مجال الجريمة المعلوماتية، حيث أوضحت الاتفاقية من خلال المادة (17) بأن على كل طرف اتخاذ الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل:

---

(1)راجع هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص172.

- التأكد من أن التحفظ العاجل لهذه البيانات المتعلقة بالمرور في تطبيق المادة(16) متوافر، بغض النظر عما إذا كان هناك مقدم خدمة واحد، أو عدة مقدمين للخدمة قد ساهموا في نقل الاتصال.
- ضمان الإفشاء السريع للسلطة المختصة، أو الشخص المعين من قبلها، عن كمية بيانات المرور الكافية التي تسمح بتحديد هوية مقدمي الخدمات، والطريق الذي تم الاتصال من خلاله.

ويشترط لتطبيق السلطات والإجراءات المشار إليها أن تكون خاضعة للمادتين (14،و15)من الاتفاقية [1].

فالمادة (17) من الاتفاقية تنشئ التزامات على الدول الأعضاء في الاتفاقية، تتعلق بالتحفظ على بيانات المرور المشار إليها في المادة (16)، كما تقرر الإفشاء السريع عن بعض بيانات المرور، بغرض تحديد هوية مقدمي الخدمات الآخرين الذين ساهموا في نقل الاتصالات.

وحداثة هذا الإجراء وكذا الإجراء السابق له، إنما كانت بهدف الوصول إلى البيانات المخزنة لفحصها قبل أن يتم التلاعب بها، وكذلك لتحديد هوية مصدر الاتصال أو منتهاه، حيث تعد من الأمور الجوهرية التي قد تقود إلى معرفة الأشخاص الذين لهم علاقة بالجريمة المعلوماتية، سواءً تعلقت بنشر مواد إباحية، أم بث فيروسات معلوماتية،

([1]) ونص المادة (17) من الاتفاقية باللغة الفرنسية

Article 17 – Conservation et divulgation rapides de données relatives au trafic

1- Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a- pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b- pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2- Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

انظر شبكة الانترنت على الربط : http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

أو الشروع أو الوصول بطريقة غير مشروعة إلى نظام معلوماتي، أو غيرها من الجرائم المعلوماتية .

وإذا كان تحديد بيانات المرور قد يبدو آمراً سهلا عندما تكون تلك البيانات مرتبطة بمقدم خدمة بمفردة، فإنها لا تبدو كذلك عندما ترتبط بأكثر من مقدم خدمة، فيحدث أن يكون عدد مقدمي خدمات قد ساهموا بنقل اتصال معين، وقد يحدث أن يحتفظ أكثر من مقدم خدمة ببيانات المرور، لأنها مرت عن طريق نظامه، وفي الغالب لا يكون بحوزة مقدم الخدمة بمفردة من بيانات المرور ما يكفي لتحديد بإتقان مصدر الاتصال ونهايته، إذ أن كل مقدم خدمة يكون لدية بعض من أجزاء اللغز، وبالتالي فإنه من جميع هذه الأجزاء التي يجب اختبارها يمكن التعرف على مصدر ومنتهى هذه الاتصالات [1].

وفي هذه الحالة عندما ترتبط البيانات بأكثر من مقدم خدمة فإن التحفظ العاجل يمكن أن يتم من خلالهم جميعا، من خلال أمر عاجل منفصل لكل مقدم خدمة على انفراد، أو أمر يشملهم جميعا ويتم إبلاغهم به بالتعاقب، أو إبلاغ البعض منهم وإلزامه بإبلاغ من يليه.

وكما تلزم السلطة مقدمي الخدمات بالتحفظ العاجل على بيانات المرور فإنها تلزمهم بالإفشاء السريع للسلطة، أو لمن تعينه من قبلها عن تلك البيانات المهمة المتعلقة بالمرور أو ببعضها، بهدف تحديد هوية كل مقدمي الخدمة الآخرين، والطريق الذي بمقتضاه تم نقل الاتصال، وبهذه الطريقة يكون بمقدور السلطة المكلفة بالتنقيب والتحري أن تحدد منبع ومصب الاتصال، وهوية أي فاعل أو فاعلين للجريمة، إلا أنه يجب من ناحية أخرى أن لا تكون تلك الإجراءات مخالفة للقيود الواردة على حقوق الإنسان وحرياته والضمانات والشروط التي نصت عليها المادتين (14،و15) من هذه الاتفاقية.

ومما يلاحظ على هذا الإجراء بالرغم من أهميته في مجال التنقيب والتحري في الجرائم المعلوماتية، أن مقدمي الخدمات قد لا يبدوا تعاونا مع الجهات أو السلطات المختصة بالتنقيب أو التحري أو التحقيق، وقد لا توجد الثقة بينهم وبين أجهزة تحقيق العدالة، ومن ثم فقد لا يكون الإجراء مفيدا بالشكل المطلوب، ويحتاج الأمر إلى اتخاذ إجراءات اشد حزما، مثل إجراءات التفتيش، أو الضبط بشرط مراعاة الحقوق المتعلقة

([1]) راجع: هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص 207.

بالخصوصية، وحقوق الإنسان بشكل عام، وبما يحقق التوازن بين إقامة العدالة والمحافظة على تلك الحقوق .

ج- الأمر بإنتاج بيانات معلوماتية

تناولت المادة(18)من الاتفاقية إجراء آخر من الإجراءات المستحدثة في مجال التنقيب والتحري والتحقيق في الجرائم المعلوماتية نظرا لطبيعتها غير المادية، ويتمثل هذا الإجراء بالتالي:

1) الأمر بتقديم (إنتاج) بيانات معلوماتية، حيث أوجبت على كل طرف في الاتفاقية تبني الإجراءات التشريعية والإجراءات التي يراها ضرورية من أجل تأهيل سلطاته المختصة أن تأمر:

- شخصا ما على أرضه بإرسال بيانات معلوماتية معينة في حوزته أو تحت سيطرته، والمخزنة في نظامه المعلوماتي، أو في دعامة تخزين معلوماتية.
- مقدم خدمات الذي قدم خدماته على أرض ذلك الطرف من أجل إرسال البيانات التي في حوزته أو تحت سيطرته والمتعلقة بالمشتركين وبتلك الخدمة.

2) يجب أن تخضع السلطات والإجراءات المقررة وفقا لهذه المادة للمادتين (14،و15) من الاتفاقية.

3) لأغراض المادة الحالية فإن تعبير البيانات المتعلقة بالمشتركين يقصد به" كل معلومات تحتوي على شكل بيانات معلوماتية، أو أي شكل آخر في حوزة مقدم الخدمة، وترتبط بالمشتركين وخدماتهم ،غير بيانات المرور والمحتوى، ويمكن من خلالها تحديد:

- نوع خدمة الاتصال المستخدمة، والأوضاع الفنية المنصوص عليها بالنسبة لفترة الخدمة.
- تحديد الهوية، والعنوان البريدي أو الجغرافي، ورقم تلفون المشترك، ورقم الولوج، والبيانات المتعلقة بدفع الفاتورة، والمبلغ المدفوع، والمتوفرة على أساس عقد أو اتفاق تقديم الخدمة.

- أية معلومات أخرى تتعلق بموقع تجهيزات الاتصال، المتوافرة على أساس عقد أو أتفاق تقديم الخدمة [1].

من خلال نص المادة سالفة الذكر يتضح بأن الاتفاقية تلزم الدول الأعضاء بأن تفرض من خلال قوانينها وسائل أخرى للتنقيبات الجنائية، أو التحقيق، اقل تدخلا في الحقوق الشخصية أو الخصوصية من إجراءات الضبط أو التفتيش، بهدف الحصول على معلومات ضرورية تفيد التنقيب أو التحقيقات، بمعنى آخر فإن أمر الإنتاج أو تقديم البيانات المعلوماتية هو: عبارة عن إجراء مرن يسمح للسلطات بأن تضعه موضع التنفيذ

([1]) المادة(18) من الاتفاقية، ونص المادة باللغة الفرنسية كما وردت في المرجع أدناه:

Article 18 – Injonction de produire

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a- à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b- à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2- Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3- Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a- le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b- l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c- toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services

انظر شبكة الانترنت على الربط : http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

هلالي عبد اللاه أحمد ،الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص211، ص212.

في حالات كثيرة، وعلى وجه الخصوص في الحالات التي لا يكون من الضروري أللجو إلى إجراء أكثر أجبارا، أو أكثر كلفة [1].

وتأسيس مثل هذا الإجراء يسهل لمقدمي خدمات الانترنت تقديم البيانات والمعلومات التي بحوزتهم تحت غطاء قانوني، حتى لا تكون أمامهم أية مسؤولية إزاء ذلك، كما أن هذا ا لإجراء لا ينطبق إلى على الشخص، أو مقدم البيانات التي تكون في حوزته، وذلك بسبب وجود مقدمي خدمات لا يحتفظون بأي اثر للمستخدمين بالنسبة لخدماتهم.

وبناء على ما سبق فإن على كل طرف أن يمكن الجهة المعنية لديه، من سلطة استصدار أمر لشخص، أو لمقدم خدمات على أرضه بأن يرسل بيانات الكترونية معينة مخزنة في نظام معلوماتي، أو دعامة تخزين معلوماتية، والتي تكون تحت حوزة أو سيطرة هذا الشخص أو مقدم الخدمات.

وتعبير" في حيازة أو تحت السيطرة " يشير إلى الحيازة المادية للبيانات المعنية داخل حدود هذا الطرف، وتشير كذلك إلى البيانات التي تكون خارج الحيازة المادية للشخص بشرط أن يكون بمقدوره السيطرة عليها، من خلال مرورها داخل حدوده، ومثال ذلك: الشخص الذي يتلقى أمر تقديم المعلومات المخزنة لحسابه عن بعد، عن طريق الخدمة الفورية للتخزين عن بعد، فيجب عليه أن يقوم بإظهار هذه البيانات في حال طلبها منه.

أما إذا كان بمقدور الشخص في الجانب التقني من الولوج إلى شبكة معينة للوصول لبيانات مخزنة عن بعد، مع أنها لم تكن تحت سيطرته القانونية، فإن ذلك لا يندرج تحت مفهوم السيطرة وفقا لما ورد في نص المادة السالف ذكرها[2].

كما أن على كل طرف في الاتفاقية أن يقيم سلطة لإصدار أمر لمقدم خدمات يقدم خدماته على أرض ذلك الطرف، بغرض إرسال البيانات المتعلقة بالمشترك والتي تكون

---

(1) هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص214.

(2) هلالي عبد اللاه أحمد، نفس المرجع، ص216

في حيازته أو تحت سيطرته، سواءً أكانت الحيازة لتلك البيانات من قبل مقدم الخدمات حيازة مادية أم عن بعد عن طريق شركة أخرى تقدم مثل تلك الخدمات[1].

ويجب أن تكون المعلومات التي يتم طلبها، هي المعلومات المتعلقة بالمشترك الذي يرتبط بالخدمات المقدمة أو الممنوحة على أرض الطرف.

ويتطلب لتحقيق هذا الإجراء النص في القوانين الداخلية للدول الإطراف على الضمانات والشروط التي تحافظ على الخصوصية وحقوق الإنسان، بحيث يمكن النص من خلال القوانين الداخلية للدول الأعضاء على اعتبار معلومات معينة في إطار السرية، كما يمكن أن تتعلق الشروط والضمانات بالسلطة التي تقوم بالإجراء بحيث يتاح لكل طرف أن ينص على السلطة المعنية باتخاذ مثل هذا الإجراء بحسب نوع البيانات المطلوب تقديمها وأهميتها، وكذلك الشخص المطلوب تقديم المعلومات عنه، فإذا كانت بيانات المشترك معروفة للعامة فيمكن أن يخول لسلطة العامة القيام بالإجراء .

بخلاف ما إذا كان الإجراء يتعلق بأمور قد تسبب في الاعتداء على الخصوصية وحقوق الإنسان فإن على الطرف أن يجعل سلطة استصدار الأمر مقتصرا على سلطة القضاء.

كما يشترط في المعلومات المطلوب تقديمها، أن تكون متصلة بالمشتركين وخدماتهم، وينصرف مصطلح مشترك إلى العديد من طوائف زبائن مقدمي الخدمات، فقد يكون الشخص الذي يدفع مقابل الخدمة، وقد يكون العميل الذي يدفع مقدما نظير الخدمات التي يستعملها، وقد يكون الشخص الذي يستخدم الخدمات مجانا، وقد يكون الذي يستخدم حساب المشترك[2].

كما يقصد بالمعلومات المتعلقة بالمشتركين وخدماتهم، البيانات المتعلقة باستخدام الخدمة ومستخدمها، وفيما يتعلق باستخدام الخدمة فتتعلق بأي معلومات باستثناء بيانات

([1]) ظهرت العديد من الخدمات التي تقدمها الشركات عبر شبكة المعلوماتية، ومن تلك الخدمات ما تقوم به شركات متخصصة في مجال حفظ البيانات المتعلقة بمؤسسات أو أشخاص، واسترجاعها في وقت الطلب، والمثير للانتباه في هذا الخصوص أن تلك الشركات قد تقع في دول غير الدول التي يقطن بها من يتم حفظ بياناتهم، ومع ذلك وباعتبار أن لا حدود جغرافية في مجال العالم الرقمي، بحيث يكون بإمكان هؤلاء استرجاع بياناتهم في وقت وجيز جدا من أماكنهم التي يقبعون فيها، بل من غرف نومهم من خلال حواسيبهم المرتبطة بشبكة المعلوماتية، فهؤلاء سواءً أكانوا أفرادا أم مقدمي خدمات فإن عليهم تقديم البيانات بما فيها البيانات المتعلقة بالمشتركين المخزنة في حواسيبهم أو التي يسيطرون عليها من بعد.

([2]) راجع: هلالي عبد اللاه أحمد، لجوانب الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص220.

المرور والمحتوى، يمكن من خلالها التعرف على نوع خدمة الاتصال المستخدمة، والبنود الفنية المتصلة بها، والفترة التي من خلالها اشترك الفرد في الخدمة.

ويقصد بالأمور الفنية: كل الإجراءات المتخذة لتمكين المشترك من الاستفادة من خدمة الاتصال المقدمة، وتضم حفظ رقم أو عنوان تقني مثل رقم التلفون، أو عنوان موقع الويب، أو اسم المجال، أو عنوان البريد الالكتروني، كذلك تقديم وتسجيل معدات الاتصال المستخدمة بواسطة المشترك، مثل الأجهزة التلفونية، أو مراكز المكالمات، أو الشبكات المحلية.

أما المعلومات المتعلقة بالمشتركين فإنها لا تقتصر على المعلومات المتصلة مباشرة باستخدام خدمات الاتصال، وإنما تعني كل المعلومات عدا بيانات المرور أو المحتوى، والتي من خلالها يتم تحديد هوية المستخدم وعنوان البريد الجغرافي، ورقم تلفونه، أو أي رقم آخر للدخول، والبيانات المتعلقة بالفاتورة أو الدفع المتوافرة على أساس اتفاقية خدمة بين المشترك ومقدم الخدمات، كذلك فإن معلومات المشتركين تعني أي معلومات ما عداء بيانات المرور والمحتوى تتعلق بالموقع والمكان الذي تتواجد به تجهيزات الاتصال المتوافرة على أساس عقد واتفاقية الخدمة، وهذه المعلومات يمكن أن تكون مفيدة من الناحية العملية عندما تكون أجهزة الاتصال غير قابله للنقل ولكن المعلومات الخاصة بنقلها أو مكانها المقترح يمكن أن يكون مفيدا في التنقيب والتحري

ومع ذلك فإن هذه المادة لا يجب أن تفهم على أنها تفرض التزاما على مقدمي الخدمات بأن يحتفظوا ببيانات حول المشتركين، أو أن يتم الطلب منهم التأكد من صحة بيانات المشتركين، وبالتالي فهم غير ملزمين بتسجيل بيانات تتعلق بهوية المستخدمين فيما يتعلق ببطاقة الدفع المسبق لخدمات التلفون المحمولة، كما لا تلزمهم المعاهدة بالتأكد من هوية المشتركين أو معارضة استخدام أسماء مستعارة عن طريق المستخدمين لخدماتهم، كما يجب أن يستخدم أمر تقديم المعلومات في قضايا فردية تتعلق في غالب الأحيان بمشترك [1]

وخلاصة ما سبق يتضح بأن الاتفاقية قد تضمنت إجراء جديدا لم تنص عليه القوانين التقليدية، يتمثل في إلزام الشخص أو مقدم الخدمات بتقديم المعلومات التي تكون

([1]) هلالي عبد أللاه أحمد، الجوانب الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق،ص223.

مخزنة في نظامه، أو تحت سيطرته إلى السلطة المختصة بموجب أمر بذلك من تلك السلطة، وهذا الإجراء يتناسب وطبيعة الدليل المعلوماتي، كمرحلة سابقة لمرحلة التفتيش والضبط تقتضيه السرعة المطلوبة التي تتطلبها الحفاظ على الأدلة الالكترونية من التلاعب بها.

د- التجميع في الوقت الفعلي لبيانات المرور

تعرضت الاتفاقية لإجراء التجميع في الوقت الفعلي لبيانات المرور كإجراء جديد لم تتضمنه النصوص التقليدية، حيث ألزمت الأطراف الموقعة عليها بالتالي :

1- تبني الإجراءات التشريعية وأية إجراءات أخرى يرى كل طرف أنها ضرورية من أجل تخويل سلطاته المختصة :

أ- جمع أو تسجيل عن طريق وسائل فنية موجودة على أرضه.

ب-إجبار مقدم الخدمات في إطار قدراته الفنية على :

1) أن يجمع أو يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه.

2) أن يعطي السلطات المختصة عونه ومساعدته من أجل تجميع أو تسجيل في الوقت الفعلي البيانات المتعلقة بالمرور مصحوبة باتصالات معينه منقولة على أرضه عن طريق نظام معلوماتي.

2- عندما لا يكون في مقدور أي طرف، بسبب القواعد الخاصة بنظامه القانوني الداخلي، أن يتبنى المبادئ المذكورة في الفقرة(1) بند (أ) فإنه بدلا من ذلك، يتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنه ضرورية من أجل التأكد من جمع أو تسجيل البيانات المتعلقة بالمرور مصحوبة باتصالات معينة منقولة على أرضه عن طريق تطبيق طرق فنية موجودة على هذه الأرض.

3- يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل إلزام مقدم الخدمات على المحافظة على أسرار الواقعة الخاصة بممارسة أي سلطة من السلطات المنصوص عليها في المادة الحالية، وكذلك كل المعلومات المتعلقة بهذا الشأن.

4- يجب أن تخضع الإجراءات المشار إليها للمادتين(14، 15) من الاتفاقية[1].

عالجت المادة السابقة مسألة التجميع والتسجيل في الوقت الفعلي لبيانات المرور كإجراءات جديدة تتناسب وطبيعة المعلومات المخزنة والمنقولة من نظام معلوماتي إلى أخر، بغرض التنقيبات والإجراءات الجنائية الأخرى.

ويعتبر إجراء التجميع الفعلي لبيانات المرور المتعلقة بالاتصالات المعلوماتية ذا أهمية كبيرة في تتبع مسار الاتصالات بين الضحية والجاني، حيث أن تقنية التنقيب والتحري المتمثلة في جمع وتسجيل بيانات المرور تسمح بعمل مقارنات بين ساعة وتاريخ و ومصدر ومآل اتصالات المشتبه به، وساعة التدخلات غير القانونية في نظم الضحايا، وهوية الضحايا الآخرين، أو بيان روابط مع شركاء آخرين[2].

وبمقتضى هذه المادة يجب الربط بين البيانات المتعلقة بالمرور واتصالات معينة منقولة، تتم على أرض الطرف المعني بالأمر، وهذه المادة تتحدث عن تجميع أو تسجيل

([1]) راجع: المادة (20) من الاتفاقية . وقد ورد النص في الفرنسي كالتالي:

Article 20 – Collecte en temps réel des données relatives au trafic

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

a- à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b- à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:

i- à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii- à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2- Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4- Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

راجع شبكة المعلومات الدولية، مرجع سابق، على الربط:

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

([2]) راجع: هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية في جرائم المعلوماتية، مرجع سابق، ص361.

البيانات المتعلقة بالمرور بصفة الجمع، وذلك يؤكد ضرورة تجميع البيانات المتعلقة بعدة اتصالات لكي يتم تحديد مصدر هذه الاتصالات وصولا إلى تحديد مرتكب الجريمة، ولا يعني ذلك قيام السلطة بتتبع الكم الهائل من بيانات المرور بهدف الوصول إلى مصدر اتصالات معينة، وإنما يجب أن تقتصر عملية الجمع والتسجيل لبيانات المرور التي لها علاقة في الكشف عن الواقعة الإجرامية.

وكما أن السلطة في الدولة الطرف في الاتفاقية تكون ملزمة بالقيام بإجراءات جمع وتسجيل البيانات المتعلقة بالمرور بموجب وسائل فنية موجودة على أرضها، على أن يسبق ذلك النص على مثل هذا في قوانينها الداخلية، فإن بإمكانها كذلك إجبار مقدم الخدمات على تجميع وتسجيل بيانات المرور، أو تقديم التعاون أو المساعدة في التجميع والتسجيل لبيانات المرور بشرط أن يكون ذلك في حدود الإمكانيات الفنية المتاحة لدى مقدم الخدمات، وفي حالة عدم توفر الإمكانات الفنية اللازمة لجمع وتسجيل البيانات لدى مقدم الخدمات، فإن تنفيذ ذلك يقع على عاتق السلطة.

كما أن تنفيذ إجراءات الجمع والتسجيل لبيانات المرور لابد وان يكون في النطاق الإقليمي للسلطة، وكذلك لابد أن تكون بعض البني التحتية والتجهيزات لمقدم الخدمات موجودة على أرض الطرف صاحب الشأن في اتخاذ الإجراء، بحيث تكون قادرة على تطبيق تلك الإجراءات، ولا يهم بعد ذلك أن تكون هذه البني والتجهيزات مقامة على موقع أخر.

ويكون الاتصال على أرض الطرف سواءً كان من يقوم بالاتصال أنسانا أم حاسبا آليا يتواجد على هذه الأرض [1].

وتجميع البيانات المتعلقة بالمرور لا تكون ذات جدوى ما لم يتم القيام بها بدون علم الأشخاص الذين ينفذ الإجراء حيالهم، لأن عملية الاعتراض سرية بطبيعتها، فكذلك يجب أن يتم الاعتراض دون علم الأشخاص الذين يقومون بالاتصال، ويجب كذلك الحفاظ على سرية اعتراض بيانات المرور من قبل مقدمي الخدمات وموظفيهم حتى يتم تنفيذ الإجراء بفاعلية.

([1])راجع هلالي عبد اللاه أحمد،الجوانب الموضوعية والجرائية لجرائم المعلوماتية، المرجع السابق ،ص364.

وحتى يتمكن أي طرف من المحافظة على سرية الإجراء، فإن عليه أن يضمن قانونه الداخلي عقوبات لكل من يقوم بتعطيل حسن سير العدالة وذلك عن طريق إعلام الجناة بموضوع الإجراء المزمع اتخاذه حيالهم.

هـ- الاعتراض في الوقت الفعلي لبيانات المحتوى

تضمنت المادة(21) من الاتفاقية النص على اعتراض البيانات الخاصة بالمحتوى[1] بقولها:

1) يجب على كل طرف أن يتبنى الإجراءات التشريعية وأي إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي – القيام بالإجراءات التالية:

أ) جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.

ب) إلزام مقدم الخدمات، في نطاق قدراته الفنية المتوافرة على :

([1]) المادة(21) من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي ،بودابست،2001. ونص المادة كما ورد باللغة الفرنسية:

Article 21 – Interception de données relatives au contenu

1- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a- à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et.

b- à obliger un fournisseur de services, dans le cadre de ses capacités techniques:

i- à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou.

ii- à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2- Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4- Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

راجع شبكة المعلومات الدولية http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

- أن يجمع، أو أن يسجل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.
- أن يمنح السلطات المختصة عونه ومساعدته من أجل تجميع، أو تسجيل في الوقت الفعلي، البيانات المتعلقة بمحتوى اتصالات معينة على أرضه، منقولة عن طريق نظام معلوماتي .

2) عندما لا يستطيع طرف ما، بسبب القواعد المقررة في نظامه القانوني الداخلي، تبني الإجراءات المشار إليها في الفقرة (1) بند(أ) فإنه يمكن أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل التأكد من أن الجمع أو التسجيل في الوقت الفعلي لبيانات محتوى اتصالات معينة على أرضه عن طريق تطبيق الوسائل الفنية المتواجدة على هذه الأرض.

3) يجب على كل طرف أن يتبنى الإجراءات التشريعية، أو أية إجراءات أخرى، يرى أنها ضرورية من أجل إلزام مقدم الخدمة بالمحافظة على سرية الواقعة، وأي معلومات عن ممارسة أي سلطة من السلطات المشار إليها في هذه المادة.

4) السلطات والإجراءات المشار إليها في هذه المادة يجب أن تكون خاضعة لإحكام المادتين14، 15 من الاتفاقية.

تبين هذه المادة بأن جمع البيانات المتعلقة بمحتوى الاتصال عن بعد يعتبر إجراء مهما، لتحديد ما إذا كان الاتصال ذا طابع غير مشروع، كأن يتضمن تهديدا، أو تأمر، أو احتيال، كما يفيد في تجميع أدلة الجرائم المرتكبة والمحتمل ارتكابها.

فارتكاب الكثير من الجرائم المعلوماتية يفترض النقل أو اتصال البيانات، وفي الغالب فإنه يصعب تحديد الوقت الفعلي للطبيعة الضارة للفعل المرتكب بواسطة المعلوماتية بدون أن يتم اعتراض محتوى الرسالة.

ويقصد بالبيانات الخاصة بالمحتوى : كل البيانات المنقولة في نطاق الاتصال غير بيانات المرور، فقد تكون بشكل رسالة، أو معلومات منقولة بواسطة الاتصال.

وخلاصة ما قيل في إيضاح المادة(20) من الاتفاقية بشأن جمع وتسجيل بيانات المرور، من الالتزام بمنح العون والمساعدة، والتزام بالسرية يمكن أن ينطبق على بيانات المحتوى، ويقتصر إجراء التنقيب في بيانات المحتوى على الجرائم الخطيرة المقرة في القانون الداخلي للدولة الموقعة على الاتفاقية .

كما أن الشروط والضمانات الخاصة باعتراض البيانات المتعلقة بالمحتوى يمكن أن تكون أكثر صرامة من تلك التي تتعلق بالتجميع في الوقت الفعلي لبيانات المرور، أو على التفتيش والضبط(1).

وقد تضمن القانون الجزائري هذا الإجراء حيث أتاح للسلطات المكلفة بالتحريات القضائية، أو سلطة التفتيش أو الحجز إمكانية وضع ترتيبات تقنية لتجميع وتسجيل محتوى الاتصالات الإلكترونية في حينها، كما جعل من ضمن التزامات مقدمي الخدمات تقديم المساعدة لتلك السلطات بهدف جمع وتسجيل محتوى الاتصالات في حينها(2).

3- حالة التفتيش أو ضبط البيانات المعلوماتية

سبق التعرض للمشاكل المتعلقة بالتفتيش أو الضبط بالنسبة لجرائم المعلوماتية وعلى وجه الخصوص التفتيش أو الضبط بصدد بيانات وبرامج الحاسوب في جانبها المنطقي، باعتبارها كيانات غير مادية، والتفتيش المنصوص عليه في القوانين التقليدية إنما اقتصر على الكيانات المادية المحسوسة.

وبسبب الخلاف الفقهي حول طبيعة المعلومات وفيما إذا كانت تعد كيانات ماديه أو غير مادية، وفيما إذا كانت تعد أموالا أو مجموعة مستحدثة من القيم إلى غير ذلك من أوجه الخلاف، الذي بسببه وجد الخلاف حول الإجراءات المتطلبة للتفتيش عليها وضبطها، وإزاء ذلك فقد وجب تحديد الإجراءات التي يمكن أن تتلاءم مع الطبيعة المنطقية لبرامج وبيانات الحاسوب، وذلك ما فعلته اتفاقية بودابست حيث تضمنت إلزام الدول الموقعة على الاتفاقية بعدد من الإجراءات منها ما يتعلق بالتفتيش، وأخرى تتعلق بضبط البيانات المعلوماتية المخزنة بنظم المعالجة الآلية للبيانات، وإجراءات الغرض منها تسهيل القيام بعملية التفتيش:

---

(1) راجع هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص272.
(2) راجع المادة (3) والمادة (10) من القانون رقم (09-04) المؤرخ في 5 غشت (أغسطس) 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أ- **فيما يخص التفتيش**

نصت عليه الفقرة(1 و2) من المادة(19) من الاتفاقية الأوربية على التالي :

1) يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تفويض سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهه:

- لنظام معلوماتي أو لجزء منه وكذلك البيانات المعلوماتية المخزنة فيه، وعلى أرضه.
- لدعامة معلوماتية تسمح بتخزين بيانات معلوماتية.

2) كما يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من اجل التأكد مما إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معين أو لجزء منه وفقا للفقرة (1) بند (أ)، وأنها تملك أسبابا تدعو للاعتقاد بأن البيانات التي تسعى إليها مخزنة في نظام معلوماتي أخر، أو في جزء منه على أرضه، وان هذه البيانات يمكن الوصول إليها بشكل قانوني سواء من خلال النظام الآلي أم من خلال كونها مهيأة من أجله، وأن هذه السلطات ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريقة مشابهة لنظام أخر[1].

([1]) الفقرتين (1،و2) من المادة(19) من الاتفاقية. وفي ما يلي نورد النص بالفرنسي.

Article 19 – Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

a- à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b- à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure= d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

انظر شبكة الانترنت على الربط : http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

وراجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص322.

ومن خلال الفقرتين(1، 2) من المادة (19) يلاحظ بأنها قد تضمنت إجراءات تتصل بتفتيش أو ضبط البيانات المعلوماتية المخزنة بهدف تجميع الأدلة، ومع أن إجراءات التفتيش أو الضبط قد تم النص عليها في جل القوانين التقليدية، إلا أنها اقتصرت على الأشياء المادية، ولأن البيانات المعلوماتية المخزنة في أنظمة المعالجة الآلية للمعطيات لا تعتبر أشياء مادية في اغلب الدول، فإن إجراءات التفتيش أو الضبط لا يمكن أن تتم بنفس طرق وتفتيش الأشياء المادية، لذلك فقد أوردت الاتفاقية نصوص قانونية تعالج مثل تلك الإشكالات.

ومع أن العديد من عناصر التفتيش التقليدية تبقى مستمرة في البيئة التكنولوجية الحديثة ومنها الشروط الخاصة من أجل الحصول على الإذن القانوني، فإن ضرورة البحث عن بيانات معلوماتية تتطلب نصوصا قانونية تكميلية من أجل أن يتم الحصول على البيانات المعلوماتية بطريقة فعالة مساوية لعملية تفتيش الدعامات المادية التي تحمل البيانات [1].

وبمقتضى المادة سالفة الذكر فإن السلطة المختصة في كل دولة طرف في الاتفاقية تكون ملزمة بموجب تشريع داخلي بالقيام بعملية التفتيش والولوج للبيانات المعلوماتية سواء الموجودة داخل نظام معلوماتي، أو في جزء منه، أو على دعامة تخزين.

وقد ورد في الاتفاقية مصطلحات جديدة تتناسب مع طبيعة الكيانات غير المادية التي يتم تفتيشها أو ضبطها، ومنها مصطلح الولوج، حيث يتناسب وطبيعة النظام والمعطيات والبرامج المدرجة فيه، مما يؤكد أن التفتيش على هذا النوع من المعطيات لابد وان تتضمنها نصوص قانونية تكميلية، إلا انه كان ينبغي أن يضاف إلى الولوج عبارة "بغرض التفتيش" وليس جعل الكلمة مرادفا للتفتيش.

وإذا كانت المادة 19 من الاتفاقية تنطبق على البيانات المعلوماتية المخزنة في النظام، فهل بالإمكان تطبيقها على الرسالة الالكترونية قبل أن يقوم المرسل إليه بإدخالها

([1]) تتطلب عملية تفتيش وضبط البيانات المعلوماتية نصوص قانونية تكميلية تتناسب مع طبيعتها الغير مادية، وذلك بسبب أنها تتوافر بشكل غير مادي وملموس، فهي عبارة عن موجات كهرومغناطيسية تحتاج إلى إجراءات من نفس طبيعتها، كما أن ضبط البيانات المخزنة يتم عن طريق النسخ مع بقاء النسخة الأصلية في النظام المعلوماتي، أو في أداة التخزين، وإجراءات النسخ غير منصوص عليها في القوانين التقليدية، وبالتالي فيجب النص عليها، كذلك فإن وجود المعلومات في نظام غير النظام المراد تفتيشه وتخزينها عن طريق هذا الأخير في النظام الأخر يتطلب توسيع عملية التفتيش من خلال نصوص تعالج مثل هذه الإشكاليات.

في نظامه المعلوماتي، أم أنها بيانات في مرحلة النقل والتحويل تنطبق عليها النصوص الخاصة باعتراض البيانات ؟

وهذا الاستفسار يتأتى في ظل وجود خلاف، حيث أن بعض التشريعات تعد الرسالة جزء من الاتصال، وأن محتواها لا يمكن الحصول عليه إلا عن طريق سلطة الاعتراض، بينما تعتبرها بعض ألأنظمة القانونية الأخرى بمثابة البيانات المخزنة التي ينطبق عليها نص المادة (19) من الاتفاقية [1].

ونرى بأن الرسالة تعتبر جزء من البيانات المخزنة بالنظام إذا كانت قد فتحت وحفظت في الحاسوب، أما إذا كانت مازالت في صندوق الوارد فهي تعتبر مخزنة في صندوق الوارد الموجود بنظام موفر الخدمات، وبالتالي فيمكن الدخول إليه وتفتيشه في حال تطلب الأمر ذلك.

كما تشير هذه المادة إلى مسألة في غاية الأهمية، وهي معالجة مشكلة الاختصاص القضائي المحلي، وذلك بالنص على توسيع نطاق إجراءات التفتيش أو الولوج بطريقة مشابهة ليشمل نظاما معلوماتيا أخر، أو جزء منه يقع على أرضه ومتصل به.

وبالتالي فإنه في حالة أن توجد أسباب تدعو للاعتقاد بأن النظام المعلوماتي الآخر أو جزء منه يحتوي على بيانات معينة يتم البحث عنها، فإن للسلطة المخولة بمقتضى القانون الداخلي للدولة الحق في تفتيش ذلك النظام أو الولوج إليه.

كما أن هذه المادة لا تعالج عملية التفتيش أو الضبط عبر الحدود، بحيث لا تتيح تفتيش نظام أو جزء منه خارج حدود الدولة.

وبالعودة للقانون الجزائري نجد بأنه قد تضمن الإجراء المشار إليه بكامل التفصيل السابق، من تخويل سلطة التفتيش الحق بتفتيش - حتى لو كان عن بعد- نظام معلوماتي أو جزء منه ، أو نظام أخر مرتبط به أو المعطيات المخزنة به، ، مع خلاف في بعض الألفاظ، حيث تضمن لفظ الدخول بغرض التفتيش، بدلا من الولوج أو التفتيش وفقا للاتفاقية، ويلاحظ بأن لفظ الدخول بغرض التفتيش أدق من لفظ الولوج دون ذكر بغرض التفتيش، حيث اعتبرت الاتفاقية بأن كلمة الولوج تحمل معنى التفتيش ، ولفظ الولوج منفردا لا يعبر عن الغرض منه وهو التفتيش فقد يقتصر الآمر على الولوج دون

---

(1) هلالي عبد اللاه أحمد،الجوانب الموضوعية والإجرائية لجرام المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23نوفمبر 2001، مرجع سابق، ص235.

القيام بالتفتيش، حيث أن إجراء التفتيش يستلزم الضبط، ومع عدم التفرقة بن لفظ الدخول أو الولوج إلا أنه كان ينبغي أن يحمل ذلك الدخول أو الولوج الغرض منه وهو التفتيش، لا أن يكون رديفا له بالمعنى كما ورد اللفظ بالاتفاقية" الولوج أو التفتيش"، ومن ناحية ثانية نلاحظ بأن الاتفاقية تتحدث عن تفتيش النظام أو النظام المرتبط به أو جزء منه، بينما في القانون الجزائري يستعمل كلمة المنظومة بدلا من النظام، وبهذا الخصوص فقد تم الإيضاح سابقا أثناء تناول جريمة الدخول والبقاء وبالتحديد عند تعريف نظام المعالجة الآلية للمعطيات بان لفظ النظام أدق من لفظ المنظومة.

كما تضمنت الاتفاقية تفتيش الدعامة المعلوماتية التي تسمح بتخزين البيانات، بينما وردت في الجزائري تحت لفظ "أو تفتيش منظومة تخزين معلوماتية" [(1)].

ب- فيما يخص إجراءات الضبط

تضمنت إجراءات الضبط في مجال المعلوماتية الفقرة(3) من المادة (19) من الاتفاقية، حيث أوجبت على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين(1،2) [(2)]، وهذه الإجراءات تشمل السلطات التالية:

- ضبط أو الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه أو إلى دعامة تخزين معلوماتية.
- التحقق والتحفظ على نسخة من هذه البيانات المعلوماتية.

---

(1) ولمزيد من تفصيل قواعد التفتيش لنظم المعلوماتية في القانون الجزائري راجع: المادة (5) من القانون رقم (09-04) المؤرخ في 5 غشت (أغسطس) 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(2)الفقرة(3)من المادة(19)من الاتفاقية الدولية بشأن مكافحة الإجرام المعلوماتي، الموقعة في مدينة بودابست،2001. والنص باللغة الفرنسية:

3- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d’une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

a- saisir ou obtenir d’une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b- réaliser et conserver une copie de ces données informatiques;

c- préserver l’intégrité des données informatiques stockées pertinentes;

d- rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

- المحافظة على سلامة البيانات المخزنة [1].

وهذه الفقرة تناقش مسألة ضبط، أو الحصول بوسيلة مشابهه على البيانات المعلوماتية كأثر من آثار التفتيش أو الولوج بطريقة مشابهه، كما تشمل ضبط الأجزاء المادية للحاسب، ودعامات التخزين المعلوماتية وذلك في حالة أن تكون خاصة النظام المعلوماتي لا تسمح بالحصول على نسخة من البيانات، ففي هذه الحالة لا يكون من حل سوى ضبط دعامة التخزين ذاتها، ونفس الأمر في حالة أن تطلب الأمر فحص الدعامة المادية لاستعادة بيانات قديمة.

كما تشمل التحقق والتحفظ على نسخة من البيانات، والمحافظة على سلامتها من التلاعب بها أو الإتلاف وبالتالي تقييد الوصول إليها من قبل المتهم، أو الغير.

وللسلطة المختصة بالتفتيش أو الضبط استخدام الوسائل التي تراها مناسبة لضبط البيانات، ومنها البرامج المعلوماتية التي تسهل من عملية الولوج إلى النظام وضبط البيانات، ولذلك فقد تم استخدام مصطلح "الحصول بطريقة مشابهه " لكي تتناسب مع ضبط البيانات غير المادية .

وبالإضافة إلى أن نص المادة (19) قد تضمن إيضاح إجراءات التفتيش أو الضبط في مجال المعلوماتية من خلال الفقرات (1، 2 ،3)، فإنه قد تضمن أيضا النص على بعض الإجراءات المسهلة لعملية التفتيش أو الضبط من خلال نص الفقرة(4)، ولم يقتصر على وضع تلك الإجراءات دون أن يحيطها بالضمانات الكافية والتي ضمنها من خلال نص الفقرة (5).

فتضمن نص الفقرة (4) بأنه: يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنه ضرورية من أجل تخويل سلطاته المختصة سلطة استصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام، أو الإجراءات المطبقة من أجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها في الفقرتين(1،2).

---

(1) راجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص413.

واخضع نص المادة (5) جميع السلطات والإجراءات التي نصت عليها المادة سالفة الذكر للمادتين (14،15) من الاتفاقية "[1].

وبناء على ماسبق فقد تضمنت الفقرة (4) إجراءً الهدف منه تسهيل عمليتي تفتيش وضبط البيانات المعلوماتية، وهي بذلك تعالج الصعوبة العملية التي يمكن أن ترافق عملية الولوج للبيانات التي يتم البحث عنها، ومطابقتها كأدلة من واقع كميات البيانات التي يتم تخزينها ومعالجتها، وهي بذلك تعطي صلاحيات للسلطة المخولة بإجراء التفتيش والضبط، بإلزام مديري النظم الذين لديهم معرفة جيدة عن النظام المعلوماتي محل البحث، بتقديم المساعدة اللازمة من أجل السماح بتطبيق إجراء التفتيش أو الضبط، إذ بدون تأكيد هذا التعاون فإن السلطات المعنية بالتفتيش والضبط يمكن أن تتأخر في الإجراءات المتخذة لفترة طويلة من الزمن مما يترتب عليه من نفقات وأعباء اقتصادية إضافية، لذلك فإن تنظيم تعاون الأشخاص المختصين يمكن أن يساعد في جعل عملية التفتيش أكثر فاعلية وأقل كلفة، وقد انعكس مثل هذا على تشريعات بعض الدول[2]، والمعلومات التي يتم إلزام مديري النظم بتقديمها تقتصر على المعلومات

([1]) الفقرة (4) والفقرة(5) من المادة(19)من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي،2001. وفيما يلي نذكر نصي الفقرتين بالفرنسي:

4- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.
5- Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

([2]) تجيز المادة(i- 125) من قانون الإجراءات الجنائية الهولندي لقاضي التحقيق أن يأمر أي شخص، يفترض فيه أنه على علم بكيفية الدخول إلى المعلومات المخزنة في الحاسبات الآلية، للمساهمة مع سلطات التحقيق في الكشف عن الحقيقة، طالما أن هذه البيانات تم تخزينها أو معالجتها، أو نقلها، عن طريق نظام المعالجة الآلية للبيانات، والأمر في هذه الحالة يقتصر على المعلومات التي استخدمت في ارتكاب الجريمة فحسب، كما تضمنت المادة (-125k) من نفس القانون الحق لقاضي التحقيق في أن يستعين أثناء التفتيش في فك شفرة نظام معلوماتي بأي شخص يفترض فيه معرفة تشغيل نظام أمن المعالجة الآلية لكي يمكنه من الدخول إلى النظام، ويتم ذلك بموجب أمر من القاضي يوجهه إلى ذلك الشخص. كما يتضمن التشريع الأمريكي قانون خاص بتعاون متعهدي خدمات الرسائل في مجال الاتصالات الالكترونية المسجلة .راجع: جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة،2002، ص107.

الضرورية فحسب، عدا في حالة أن يكون من شأن ذلك الإجراء- تقديم البيانات- تهديد الحياة الخاصة لمستخدمين آخرين أو لطابع السرية بشكل غير مقبول[1].

أما الفقرة(5) من المادة (19) فقد ألزمت السلطات المختصة بمراعاة بعض الضمانات أو الشروط التي يجب مراعاتها أثناء التفتيش أو الضبط وفقا لنصي المادتين (14، 15) من الاتفاقية والتين تضمنتا مراعاة الحق في الخصوصية وحقوق الإنسان أثناء القيام بأي إجراء مما نصت عليه الاتفاقية.

ولبحث ما إذا كان من اللزوم إخطار الأطراف المعنية بحضور التفتيش، أثناء القيام بالتفتيش عن الآثار المعلوماتية، أسوة بالتفتيش عن الأشياء المادية وفقا لما تضمنته اغلب القوانين التقليدية، فتترك المسألة لتقدير القاضي المختص بإصدار إذن التفتيش بحسب كل حالة على حدة، بحيث تخضع للتقدير الموضوعي للحالة نفسها، فإذا اقتضت الضرورة عدم أو تأجيل الإخطار فيخول القاضي بإصدار الإذن ويضمنه التأجيل، أو عدم الإخطار، بخلاف الوضع العام التي لا توجد فيه حالة ضرورة أو استعجال فلابد من إخطار من له علاقة بالتفتيش أسوة بالقواعد التقليدية.

وقد تلافى المشرع الجزائري قصور إجراءات الضبط في مجال المعلوماتية وفقا للنصوص التقليدية ووضع قواعد خاصة بالضبط تتقارب من القواعد المشار إليها في الاتفاقية، وقد تم إيضاحها أثناء تناول المشاكل الإجرائية المتعلقة بالضبط لسنا بصدد تفصيلها تلافيا لعدم التكرار.

---

(1) راجع: هلالي عبد اللاه أحمد، الجوانب الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست بشأن مكافحة الإجرام المعلوماتي، مرجع سابق، ص242.

المطلب الثاني

مكافحة الجرائم المعلوماتية ذات البعد الدولي

اثبت الواقع أن أي دولة لا تستطيع بجهودها أن تقضي على الجرائم المعلوماتية، وتلاحق مرتكبيها وتتابع الأدلة المتعلقة بشأنها، بسبب التطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات، بالإضافة إلى ظهور الإنترنت والانتشار الواسع والسريع لها، والذي أدى إلى ظهور أشكال وأنماط جديدة من تلك الجرائم، والتي أضحت تشكل خطرا على سرية وسلامة البيانات والنظم، وتعدت تلك الخطورة الحدود فيما بين الدول، فأصبحت تلك الجرائم تهدد المجتمع الدولي بأسره، وغالبا ما يتم ارتكاب الجريمة الواحدة بأكثر من دولة، مثلها مثل الجريمة المنظمة التي عبرت الحدود الجغرافية منذ زمن بعيد للتحول إلى ظاهرة عبر وطنية(1).

ولمكافحة جرائم المعلوماتية ذات البعد الدولي، وعلى وجه الخصوص المرتكب منها عن طريق الشبكات، فإن الأمر يتطلب توحيد التشريعات المختلفة من ناحية، وأن يكون نظام الإثبات بالدليل الالكتروني واحداً بين الدولة التي وقعت فيها الجريمة، والدولة التي يقيم المتهم فيها وتتولى المحاكمة عنها، وهذا أمر مستحيل تحقيقه (2)، ولذلك لابد من وجود تعاون دولي لمكافحة تلك الجرائم وآليات يتم من خلالها تحقيق ذلك التعاون سواء من حيث تبادل الخبرات والمعلومات بين الأجهزة المختصة في الدول الأطراف وكيفية تعقب الجناة وتتبعهم وتسليم المجرمين وما إلى ذلك من صور التعاون(3).

وبهذا الخصوص فقد أُبرمت العديد من الاتفاقيات الدولية بهدف التقريب بين القوانين من أجل مكافحة الجرائم العابرة للحدود ومنها الجرائم المعلوماتية، ومن تلك المعالم التي أقرتها الاتفاقيات، قبول حالات تفويض الاختصاص في اتخاذ إجراءات

---

(1) محمد سامي الشواء، الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية،1998، ص199، منير محمد الجنبيهي ومحمود محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي، الإسكندرية،2004،ص110.

(2) جميل عبد الباقي الصغي، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص72. وراجع:
Solange Ghernaouti –Hélie, Sécurité Informatique et réseaux, dunod, paris, 2006, P.31.

(3) موسى مسعود أرحومة، الإرهاب والانترنت، بحث مقدم إلى المؤتمر الدولي بجامعة الحسين بن طلال، الأردن، حول الإرهاب في العصر الرقمي، ت.د 10/ /3 2007، منشور على شبكة المعلومات الدولية،على الربط:
http://www.ipcciraq.org/alhallmg/print.php?id=274

التحقيق وجمع الأدلة، وتسليم المجرمين، والاعتراف بالأحكام الجنائية الأجنبية، سوف نتطرق باختصار إلى أهمها:

1- التعاون القضائي

تتأتى أهمية التعاون القضائي في مجال مكافحة الإجرام المعلوماتي، بسبب وجود العديد من الصعوبات التي لها علاقة بتلك الجرائم ومنها صعوبة تحديد هوية مرتكبي هذا النوع من الجرائم، وصعوبة إثباتها ونسبتها إلى مرتكبها، في ظل عالميتها وتخطيها للحدود فيما بين الدول، وكذلك المشكلات المتعلقة في كيفية استيراد البيانات التي تم تخزينها عن بعد في حالة اعتبارها دليل إثبات، حيث لا توجد قاعدة عامة لحل هذه المشكلة [1]، دون تعاون أو مساعدة قضائية.

كما أن القرارات التي تصدر من المحاكم بالنسبة لهذه الجرائم لا يمكن فرضها على دول أخرى غير التي صدرت بها، ولا يترتب عليها أي أثر قانوني ما لم تعترف بها الدول الأخرى[2].

وتعرف المساعدة القضائية الدولية بأنها: كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخري بصدد جريمة من الجرائم [3].

ولتحقيق ذلك فإن مجلس وزراء أوربا قد دعا إلى إيجاد تعاون دولي في مجال تفتيش أجهزة الكمبيوتر[4]. كما تضمنت الاتفاقية الأوربية لمكافحة الإجرام المعلوماتي على عدد من الإجراءات المستحدثة في إطار التعاون الدولي، بالإضافة إلى الصور التقليدية للتعاون الدولي سوف نشير إلى أهمها:

أ- **التعاون القضائي في الجانب الجنائي بشكل عام**

للتعاون القضائي في المجال الجنائي عدة صور منها:

- **تبادل المعلومات:** ويشمل هذا الإجراء تقديم المعلومات والبيانات والوثائق التي لها

---

(1) عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها، مرجع سابق، ص132.

(2) Boudoumi Abderrahmane, op. cit., p.5.

(3) سالم محمد سليمان الاوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس،1997م ص 425 .مشار إليه لدى جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص79.

(4) ومن ذلك أن المجلس الأوربي يدعو أعضاءه إلى التعاون في مجال تفتيش الأنظمة المعلوماتية، بحيث يستطيع رجال الضبط القضائي تفتيش النظم المعلوماتية المتواجدة في دول أخرى، مع مراعاة سيادة تلك الدول، وفي سبيل تحقيق ذلك تدعو لجنة الوزراء بالمجلس الأوربي إلى إيجاد أساس قانوني صريح ينظم التفتيش للأجهزة الممتدة إلى الدول الأخرى.راجع: شيماء عبد الغني محمد عطا الله، مرجع سابق، ص330.

علاقة بالاستدلال ، أو التحقيق للسلطة القضائية ألأجنبية، أثناء نظرها لجريمة ما، وقد تضمنت هذه الصورة العديد من الاتفاقيات الدولية، أهمها معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[1].

- كما يوجد لها تطبيق كذلك في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية2000 في البنود الثالث والرابع والخامس من المادة الثامنة منها[2].
- **نقل الإجراءات:** ويقصد به قيام دولة ما باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة متى ما توافرت شروط معينة من أهمها التجريم المزدوج، وأن تكون الإجراءات المطلوب اتخاذها مقره من قبل الدولة المطلوب منها اتخاذها، كما يشترط أن تكون الإجراءات المطلوب اتخاذها مهمة في الوصول إلى الحقيقة [3].
- **الإنابة القضائية الدولية:** ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها

---

(1) راجع: الفقرة(2)من المادة(1) من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية والتي تقضي باتفاق أطرافها على أن يقدم كل منهم للأخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات، أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة.راجع : حسين بن سعيد بن سيف الغافري، مرجع سابق، منشور على الشبكة المعلوماتية على الرابط: صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة

www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014

(2) وتطبيقا لمبدأ تبادل المعلومات ونقل الإجراءات، ما قامت به السلطات المصرية من تعاون مع قسم جرائم الحاسبات بالولايات المتحدة الأمريكية بجهاز المباحث الفدرالية الأمريكية (FPI) من تبادل معلومات، وضبط عدد (25) متهم من عدد 47 مشتبه مصري، وكذلك ضبط عدد 33 متهم من 53 أمريكي، لأكبر تشكيل عصابي مصري أمريكي، قاموا بالدخول على ثلاث صفحات لثلاثة بنوك أمريكية، وحصلوا على بيانات بعض العملاء، ومن ثم قاموا بالتواصل معهم على اعتبار أنهم مسؤولين في البنوك الثلاثة، وطلبوا منهم إرسال أسماؤهم ورقم بطائق الائتمان الخاصة بهم عن طريق البريد الإلكتروني لتأكيدها، وحصلوا بذلك على ملايين الدولارات، بعد التنسيق مع أمريكيين تم التعرف عليهم عن طريق الشات بالإنترنت، وتم الاتفاق معهم، على عمل حسابات وهمية بأسمائهم لكي يقوم المصريين بتحويل الأموال التي تم الحصول عليها بالتحايل لتلك الأسماء، ويتقاسموا المبلغ فيما بعد بينهم بموجب النسب التي تم الاتفاق عليها، حيث كان الأمريكيون بعد حصولهم على المبلغ يحولون النسبة الخاصة بالمصريين، فهذه القضية كان للتعاون الدولي دور- أن لم يكن في كشفها لكون السلطات الأمريكية هي التي كشفت تفاصيلها - ففي متابعتها وضبط أطرافها. راجع موقع جريدة الحوادث المصرية، وموقع وزارة العدل الأمريكية، ت.د 2009/11/11 على الرابطين:

http://www.alarab.com.qa/admin/pdf/files/1556339366_Hawadeth1.pdf
http://www.justice.gov/criminal/cybercrime/cc.html#CC

(3)راجع: المادة (21) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية،2000.

القيام به بنفسها [1]، وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيرها، وفي العادة يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، ومن ثم يتم إرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب، إلا أنه يحدث أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية – عادة ما تكون وزارة العدل- ترسل إليها الطلبات مباشرة بدلا من الولوج إلى القنوات الدبلوماسية والتي من شأنه تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما لو تم عبر تلك القنوات[2]، وفي القانون اليمني يكون ذلك في حالة الاستعجال[3].

ب- التعاون القضائي في مجال جرائم المعلوماتية

نظرا للأهمية التي لعبتها جرائم المعلوماتية في تعدي الحواجز والحدود في ما بين الدول، وعدم استطاعة الدول بشكل منفرد من السيطرة عليها، وبسبب عدم كفاية التعاون الدولي وفقا للنصوص التقليدية- بالرغم من أهميتها- في مكافحة جرائم المعلوماتية، فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق من خلال بعض الإجراءات الجديدة ومنها:

1) طلب الحفظ السريع للمعلومات

تضمنت الاتفاقية الدولية لمكافحة الإجرام المعلوماتي النص على سرية البيانات المخزنة، و أجازت لكل طرف موقع عليها بأن يطلب من الطرف الأخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الالكترونية الموجودة داخل النطاق المكاني لذلك

(1)جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص83.
(2)المادة(2) من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990م.راجع: حسين بن سعيد بن سيف ألغافري، مرجع سابق، منشور على الشبكة المعلوماتية على الرابط:
www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014
(3) راجع: حسن علي مجلي، المحاكمة في قانون الإجراءات الجزائية اليمني، بدون ذكر دار النشر ورقم الطبعة، 2001، ص20.

الطرف، والتي ينوي الطرف طالب المساعدة أن يقدم طلباً للمساعدة بشأنها بغرض القيام بالتفتيش، أو الدخول بأي طريقة مماثلة، وضبط، أو الحصول، أو الكشف عن البيانات المخزنة في نظام المعالجة الآلية للبيانات [1].

([1]) راجع المادة(29) من الاتفاقية الدولية للإجرام المعلوماتي، الموقعة في 2001. وفيما يلي النص باللغة الفرنسية:

Article 29 – Conservation rapide de données informatiques stockées

1- Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2- Une demande de conservation faite en application du paragraphe 1 doit préciser:

a- l'autorité qui demande la conservation;

b- l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c- les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d- toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e- la nécessité de la mesure de conservation; et

f- le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3- Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4- Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5- En outre, une demande de conservation peut être refusée uniquement:

a- si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b- si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6- Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7- Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

2) طلب الكشف السريع عن البيانات

أكدت الاتفاقية الدولية لمكافحة الإجرام المعلوماتي على حق الدول الأطراف فيها من طلب الكشف السريع عن البيانات التي تم حفظها، حيث نصت على (أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة، والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29، فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال، فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله)[1].

3) التفتيش والضبط والكشف عن البيانات

تضمنت الاتفاقية الدولية لمكافحة الإجرام المعلوماتي كذلك النص على المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش، أو أن يدخل بأي طريقة مشابهة، وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف، والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة (29)، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية[2]:

([1]) المادة(31) من الاتفاقية الدولية للإجرام المعلوماتي. وفيما يلي نورد النص بالفرنسي:

Article 31 – Entraide concernant l'accès aux données stockées

1- Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2- La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3- La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a- il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b- les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide

([2]) راجع المادة(30) من الاتفاقية الدولية للإجرام المعلوماتي، وفيما يلي نورد النص بالفرنسي كما ورد في الموقع الإلكتروني أدناه:

Article 30 – Divulgation rapide de données conservées

1- Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux=

1- إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة لمخاطر الفقد أو التعديل.

2- أن الوسائل والاتفاقات والتشريعات الواردة في الفقرة 2 تستلزم تعاوناً سريعاً.

4) الدخول وجمع البيانات المخزنة خارج الحدود

كما أن من الإجراءات الجديدة التي تضمنتها الاتفاقية الدولية لمكافحة الإجرام المعلوماتي السماح للدول الأطراف بالدخول للبيانات المخزنة خارج نطاق الحدود، بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور(1).

فملاحقة مرتكبي تلك الجرائم، وتقديمهم للمحاكمة، وتوقيع العقاب عليهم، يستلزم في الغالب القيام بإجراءات قد تتمثل تلك الإجراءات المطلوب اتخاذها- في ظل المساعدة القضائية- في معاينة مواقع الإنترنت في الخارج، أو تفتيش الوحدات الطرفية في حال الاتصال عن بعد.

كذلك فقد تضمنت الاتفاقية النص على تعاون الدول الأطراف فيما بينها، لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وينظم هذا التعاون الشروط والإجراءات المنصوص عليها في القانون الداخلي، ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جمع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة

=fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2- La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:

a- si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b- si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité,

(1) راجع المادة (32) من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي، بودابست، 2001. والنص بالفرنسي:

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

a- accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b- accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

على المستوى المحلي[1].

5) التقاط البيانات

يوجد كذلك من الإجراءات الجديدة في مجال التعاون الدولي بخصوص مكافحة جرائم المعلوماتية، السماح للدول الأطراف في التقاط البيانات التي لها علاقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات[2].

ويلاحظ مما سبق أن الاتفاقية الأوربية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بشبكة الإنترنت.

وفي ما يخص دور القانون الجزائري في مجال التعاون والمساعدة القضائية الدولية إزاء جرائم المعلوماتية يلاحظ بأنه قد لاحق التطور في التشريعات في هذا المجال، ولم يكتفَ بالقواعد العامة المنصوص عليها في القوانين التقليدية والتي كانت تخص الجرائم المادية.

وبهذا الخصوص فقد تضمن القانون الجزائري لعام 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال الفصل السادس والأخير، ما يتعلق بالتعاون والمساعدة القضائية الدولية.

---

(1) راجع: المادة (33)من الاتفاقية ، وللرجوع إلى نص المادة باللغة الفرنسية ،يتم الرجوع إلى الموقع أدناه ،حيث ورد النص كالتالي:

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1- Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.
2- Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

(2) راجع نص المادة(34) من اتفاقية بودابست، بشأن مكافحة الإجرام المعلوماتي،2001. وفيما يلي نذكر النص بالفرنسي:

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

وراجع حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، بحث منشور على شبكة الانترنت، ص43.ص44. موقع المنشاوي ،على الربط :

www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014

حيث تضمنت المادة (16) منه المساعدة القضائية الدولية المتبادلة، وقد ورد النص كالتالي (في إطار التحريات، أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة لقضائية الدولية، لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبادئ المعاملة بالمثل قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها) [1].

كما تضمنت المادة (17) الكيفية التي تتم بها تبادل المعلومات واتخاذ الإجراءات التحفظية بين الجزائر وغيرها من الدول التي تخزن في أنظمتها معلومات تفيد في كشف غموض الجريمة، حيث ورد النص (تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات، أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة، أو الاتفاقات الدولية الثنائية ومبادئ المعاملة بالمثل)[2].

والمشرع الجزائري إذ نظم الإجراءات التي تتم بواسطتها المساعدة القضائية وتبادل المعلومات بين الجزائر والدول الأخرى، لم يجعل ذلك التعاون مطلقا بل قيده ببعض القيود التي من شأنها المحافظة على السيادة الوطنية والمحافظة على سرية المعلومات، وذلك من خلال نص المادة (18) حيث جاء النص على النحو التالي(يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو لنظام العام.

يمكن، أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة، أو بشرط عدم استعمالها في غير ما هو موضح في الطلب)[3].

كما أن المشرع الجزائري علاوة على ما ذكر من تبادل المساعدة القضائية والمعلومات بين السلطات المختصة في الجزائر والدول الأخرى، قد جعل من مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

([1]) المادة (16) من القانون رقم (09 -04) المؤرخ في 5 غشت (أغسطس) 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(2) المادة (17) من نفس القانون.

(3) المادة (18) من القانون رقم (09 -04) المؤرخ في 5 غشت (أغسطس) 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[1].

وبناء على ما سبق يتضح بأن القانون الجزائري قد حاول من خلال النصوص المشار إليها أن يسهل من إجراءات التعاون القضائي الدولي بما يتناسب مع مكافحة جرائم المعلوماتية، حيث يتطلب لمكافحتها وكشف غموضها السرعة في الإجراءات الفنية والتقنية، ومن تلك الإجراءات:

- تخويل السلطات المختصة الحق في تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية وكشف مرتكبيها.
- يمكن قبول طلبات المساعدة القضائية في حالة الاستعجال عن طريق وسائل الاتصالات السريعة بما فيها البريد الإلكتروني وأجهزة الفاكس، بشرط المعاملة بالمثل، ومع مراعاة الاتفاقيات الدولية.
- إقرار مبدأ المعاملة بالمثل وكذلك الاتفاقيات الدولية الموقع عليها من قبل الجزائر، لتبادل المعلومات واتخاذ الإجراءات التحفظية - بهدف كشف الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال ومكافحتها- بين السلطات المختصة بالجزائر والدول الأخرى.

اما القانون اليمني فلم يتضمن نصوص مستحدثة تتضمن التعاون القضائي الدولي في مكافحة جرائم المعلوماتية، واقتصر الآمر على النصوص التقليدية الخاصة بالإنابة القضائية، والتي بمقتضاها يجوز للنيابة العامة أو المحكمة أثناء نظر الدعوى، أن تنيب أحدى السلطات الأجنبية في اتخاذ إجراء، أو أكثر من إجراءات التحقيق الابتدائي أو النهائي، وتوجه هذه الإنابة إلى وزارة الخارجية لتبليغها بالطرق الدبلوماسية، ويجوز في أحوال الاستعجال أن توجه الإنابة مباشرة إلى السلطة القضائية الأجنبية المطلوب منها القيام بالإجراء، وفي هذه الحالة يجب أن ترسل صوره من الإنابة القضائية مصحوبة بجميع الوثائق إلى وزارة الخارجية لتبليغها بالطرق الدبلوماسية.

([1]) راجع: الفقرة (ج) من المادة (18) من نفس القانون.

كما أن على النيابة العامة أو المحكمة أن تقبل الإنابة القضائية التي ترد إليها بالطرق الدبلوماسية من أحدى السلطات الأجنبية ، ويجري تنفيذها وفقا للقواعد المقررة في القانون اليمني.

ولا يجوز إبلاغ نتيجة الإجراء إلى السلطات الأجنبية قبل وصول الطلب الرسمي بالطريق الدبلوماسي إذا كانت الإنابة قد وجهت مباشرة [1].

فهذه النصوص تتضمن إجراءات لا تتسم بالسرعة التي تتطلبها مكافحة الجرائم المعلوماتية، بحيث يتم تبادل الإنابة عن طريق إجراءات رسمية تقليدية عبر وزارة الخارجية، وذلك قد يستغرق وقتا طويلا يساعد على محو اثأر الجريمة أو التلاعب بها، لأنها عبارة عن أدلة ذات طبيعة معنوية سهلة الإخفاء والتلاعب.

كما أن النص المتضمن عدم التقيد بالإجراءات الرسمية، بحيث يمكن قبول طلبات المساعدة القضائية عن طريق الجهات القضائية المختصة فيما بينها دون مرور تلك الطلبات عن طريق الخارجية، لم يتضمن استخدام وسائل الاتصال السريعة مثل البريد الالكتروني أو الفاكس.

وبالتالي فإن على المشرع اليمني أن يحذو حذو التشريعات الحديثة والاتفاقات الدولية في مجال الوقاية من جرائم المعلوماتية ومكافحتها، وعدم إهمال ما يخص التعاون الدولي في مكافحة ذلك النوع من الإجرام والوقاية منها.

2- تسليم المجرمين

يقوم مبدأ تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود، ومنها جرائم المعلوماتية، عليها أن تحاكمه إذا كان تشريعها يسمح بذلك، وإلا فإن عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى[2].

ويشترط في الغالب لتطبيق مبدأ تسليم المجرمين ازدواجية التجريم في الدولة طالبة التسليم والدولة المطلوب منها التسليم، ويشترط كذلك لتطبيق المبدأ أن يكون قانون الدولة طالبة التسليم مختصا بمحاكمة الشخص المطلوب تسليمه إليها، وبالمقابل يتعين أن لا

([1])راجع: المواد (252، 253) إ.ج.ي رقم (13) لسنة 1994.
([2]) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص88.

يكون قانون الدولة المطلوب منها التسليم مختصا بمحاكمة الشخص المطلوب تسليمه عن ذات الفعل المنسوب إليه ارتكابه.

ومع ذلك فإن شرط ازدواجية التسليم يتحول إلى عائق في مجال تسليم المجرمين، لكون جرائم المعلوماتية هي في حقيقتها جرائم مستحدثة غير معاقب عليها بصورة صريحة في اغلب التشريعات الوطنية، ومن الصعب التحقق فيما إذا كان بالإمكان تطبيق النصوص التقليدية في الدول طالبة التسليم على جرائم المعلوماتية المطلوب تسليم المجرمين بشأنها، ولذلك يجب أن يكون هناك تنسيق بين التشريعات المختلفة بتعريف الجرائم المعلوماتية، أو يتم التخلي عن شرط ازدواجية التجريم.

كذلك فقد امتد التعاون الدولي في مجال مكافحة الجريمة المعلوماتي عبر الانتربول فلم يقتصر دوره على مكافحة الجرائم التقليدية، المنصوص عليها في القوانين التقليدية في إطار التعاون الأمني بين الدول، بل إن نشاط تلك المنظمة قد أمتد ليشمل التعاون الدولي في مكافحة جرائم المعلوماتية في إطار تلك المنظمة، من خلال إنشاء وحدة لمكافحة جرائم التكنولوجيا، ووضع استراتيجيات لمكافحة تلك الجرائم من خلال أنشا مركز اتصالات يعمل على مدى 24 ساعة للتواصل، وتزويد الدول بالكتيبات الإرشادية التي توضح كيفية التعامل مع تلك الجرائم، وحث الدول على استخدام وسائل حديثة في المكافحة، وقد أمتد نشاط المنظمة في مجال التعاون الدولي إلى تحقيق بعض الإنجازات في مجال كشف بعض جرائم المعلوماتية وصولا إلى ضبط مرتكبيها(1).

وفي مجال التعاون الدولي المحدود في مجال الاتحادات الدولية التعاون الذي يتم بين دول الإتحاد الأوربية تحت أشراف عدد من الأجهزة المتخصصة التي تم تأسيسها لهذا الغرض، ومنها الاوربول (2) .

---

(1) ومن تلك الإنجازات التي حققتها منظمة الانتربول الدولي في مجال التعاون الدولي لمكافحة جرائم المعلوماتية، التعاون في ملاحقة الشخص الذي قام بنشر دودة الحب عبر الإنترنت من الفلبين وتسببت في تدميرعدد كبير من بيانات وأنظمة الحواسيب في الولايات المتحدة الأمريكية، حيث تمكنت المباحث الفدرالية الأمريكية (FPI بالتعاون مع الانتربول والسلطات الفلبينية من الوصول إلى المتهم وضبطه. كذلك فقد استطاعت المباحث الفدرالية الأمريكية مع الشرطة الانجليزية عن طريق الانتربول من تفكيك موقع منشور عليه أكثر من 75.000 صورة دعارة أطفال والقبض على 107 أشخاص في 12 دولة. راجع: نبيله هبه هروال، الجوانب الإجرائية لجرائم الإنترنت، رسالة ماجستير، ط1، دار الفكر الجامعي، الإسكندرية ،2007،ص158.

(2) و الاوربول - مركز الشرطة الأوربية- هو أحد الأجهزة المتخصصة على مستوى الدول الأوربية، وله عدة مهام منها تسهيل تبادل المعلومات، كما أن له دور فعال في مكافحة جرائم الإنترنت، حيث يعمل على تسهيل التحقيقات في تلك الجرائم بين دول الاتحاد الاوربي، ومن تلك الجرائم جرائم بث أو امتلاك محتويات إباحية عبر الإنترنت. راجع نبيله هبه هروال، المرجع السابق، ص159.

وخلاصة ما سبق يتضح في أن الاتفاقيات والتوصيات الدولية وأهمها الاتفاقية الدولية للإجرام المعلوماتي، قد تضمنت حلولا إلى حد ما للمشكلات الإجرائية في مجال مكافحة الجرائم المعلوماتية فيما يتعلق بالاستدلال، أو التحقيق أو الاختصاص القضائي، وغير ذلك من الإجراءات، على مستوى إقليم الدولة، أو على المستوى الدولي.

بالإضافة إلى إيجاد إجراءات مستحدثة لم تكن القوانين التقليدية تتضمنها حتى تتناسب مع طبيعة الجرائم المذكورة والوسائل المرتكبة بواسطتها، ومن تلك الإجراءات التقاط المعلومات، واعتراضها، والولوج إليها، والتحفظ عليها، وتجميعها وتبادلها بين الدول الأطراف، وغيرها من الإجراءات التي تسهل عملية الملاحقة، وكشف تلك الجرائم.

ومع ذلك فلم يطلق العنان للسلطات المختصة في اتخاذ تلك الإجراءات، بل أن ذلك مشروط بعدد من الشروط والضمانات التي تضمنتها تلك الاتفاقيات، وألزمت الدول الأطراف بمراعاتها أثناء القيام بأي إجراء مما ذكر، وجميعها تتعلق بحماية الحق في الخصوصية، وكذلك كافة الحقوق المنصوص عليها في المواثيق والمعاهدات الدولية الخاصة بحقوق الإنسان .

الخــاتـمـة:

تضمنت هذه الدراسة في مضمونها إيضاحاً لأهم الجرائم المعلوماتية في القانونين اليمني والجزائري، والمشكلات الإجرائية المترتبة عليها، والتعاون الدولي في معالجة تلك المشكلات، من خلال الاتفاقيات والتوصيات الدولية، ونظراً لحداثة الموضوع، فقد تلقينا صعوبات مختلفة سواءً في الشكل أم المضمون وتظهر في: الأفكار التقنية والعلمية التي لم تتضمنها القوانين الجنائية التقليدية، وكذلك مشكلة اللغة كون المراجع المتخصصة في دراسة هذا النوع الجديد من الإجرام هي في حقيقتها مراجع أجنبية، وكذلك فإن القوانين التي سبقت في تنظيم التعامل مع تلك الجرائم موضوعياً وإجرائياً هي قوانين أجنبية، وما المراجع العربية وكذا القوانين إلا مستسقاة من تلك المراجع والقوانين الأجنبية، إضافة إلى ضعف الترجمة في المراجع العربية.

وقد اتضح من خلال هذه الدراسة أن القوانين الجنائية الموضوعية والإجرائية التقليدية لا تفي لمواجهة تلك الجرائم، كما أن التشريعات الحديثة بما فيها القانون الجزائري مازالت قاصرة في مواجهة أغلب الجرائم ومنها الجرائم المتعلقة بالإنترنت، ولذا فإن القانون الصادر في 2004 لم يطبق من طرف المحاكم الجزائرية، مما جعل الجهات القضائية ترجع إلى التكييفات التقليدية حتى إذا تعلق الأمر بالأفعال المرتكبة عن الإعلام الآلي والإنترنت، وهذا ما أدى إلى انعدام القضاء في هذا الميدان.

وأما القانون اليمني فمازال حتى الانتهاء من إعداد هذه الاطروحة خال من نصوص لمواجهة تلك الجرائم موضوعياً وإجرائياً .

ويتضح كذلك بأن القوانين التي نصت على تلك الجرائم وتبنت مواجهتها موضوعياً وإجرائياً ومنها التشريع الجزائري لا تكفي لمواجهتها، ما لم توجد إستراتيجيات مكملة على المستوى الفني التقني والقضائي، وتحديث الآليات التقليدية على مستوى التعاون القضائي الدولي وتسليم المجرمين. ففي ضوء ما سبق وبعد الاطلاع والمقارنة لعدد من القوانين والاتفاقيات الدولية وعلى رأسها القوانين الجزائرية ذات العلاقة بالموضوع، كان من ضمن أهداف هذه الدراسة، تنبيه المشرع اليمني لما يجب أن تشتمل عليه النصوص القانونية، أثناء إعداد مشروع قانون لمكافحة ومواجهة جرائم المعلوماتية موضوعياً وإجرائياً ، أو إضافة تلك النصوص إلى قانون العقوبات والإجراءات، تمشياً

مع القوانين الحديثة في هذا المجال، وكذلك بيان بعض الأمور التي يمكن للمشرع الجزائري الأخذ بها في تبني وإدخال التعديلات اللازمة في قانون العقوبات والإجراءات الجنائية بما يتناسب والتعامل مع تلك الجرائم أثناء مكافحتها وكشفها وضبطها وصولا إلى سن العقوبات التي تتناسب معها.

وقد أظهرت الدراسة عدداً من النتائج التي في ضوئها سيتم تبني عدد من المقترحات التي تعالج تلك المشكلات، وتتجلى في النقاط التالية:

1. إن جرائم التكنولوجياالمعلوماتية كانت ومازالت محلاً للخلاف الفقهي والقضائي، بالنظر إلى قيمة المعلومات، وطبيعتها غير المادية، ومدى تحقق صفة المال فيها، وتملكها، كذلك في إجراءات التفتيش والضبط عن بعد، وطبيعة الأدلة الناتجة عنها، وتعديها للحدود الجغرافية، وشرعية الحصول على الأدلة الناتجة عنها والعمل بها، وتحديد نطاق الاختصاص المكاني المحلي والدولي والقانون واجب التطبيق، ومدى كفاية النصوص التقليدية موضوعية كانت أو إجرائية لمواجهتها، خاصة في الدول التي مازالت لم تعدل من قوانينها، أو تصدر قوانين حديثة لمواجهتها.
2. أظهرت الدراسة أن هناك قصوراً واضحاً في التشريع اليمني بشقيه الموضوعي والإجرائي، فلم يتضمن نصاً قانونياً واحداً ينظم الحماية الجنائية من الجرائم المعلوماتية سواءً المستحدثة منها، أم التقليدية المرتكبة بواسطة النظم المعلوماتية، ووسائل وإجراءات مكافحتها ضمن نصوص قانون العقوبات والإجراءات، كذلك لم يسن قانوناً خاصاً لمواجهة تلك الجرائم، ولذلك فإن القانون التقليدي هو المعمول به على الرغم من المشكلات التي قد تحول دون تطبيق نصوصه، ومن ذلك:

- لم ينص على جريمة الدخول إلى نظام المعالجة الآلية للبيانات أو البقاء فيه، لا بصورتها البسيطة ولا المشددة، ولا يمكن قياس ذلك على الدخول إلى مسكن، لأن الدخول في الأولى دخول معنوي تستخدم فيه التقنية الحديثة، وفي الثانية دخول مادي ملموس.
- عدم النص على جريمة التلاعب العمدي بالمعطيات، وكذلك جريمة إتلاف نظام المعالجة الآلية للبيانات، ولا يمكن تطبيق عقوبة جريمة الإتلاف المادية على ذلك.

- عدم النص على جرائم التعامل بالبيانات التي يمكن أن ترتكب بها الجرائم المعلوماتية، أو البيانات الناتجة عن ارتكابها.
- عدم تضمين القانون الجرائم المعلوماتية عندما تستهدف مؤسسات الدفاع الوطني والهيئات الخاضعة للقانون العام، وتشديد العقوبات على اقتراف تلك الجرائم.
- عدم تجريم وتشديد العقوبات لجرائم المعلوماتية عندما يتم اقترافها من الشخص المعنوي.
- عدم النص على أي من الجرائم المتعلقة بالإنترنت.
- عدم وجود نصوص قانونية إجرائية تتعلق بتمديد الاختصاص المكاني بهدف القيام بالإجراءات الخاصة بكشف تلك الجرائم ومرتكبيها، وكذلك التفتيش عن بعد، ووضع الترتيبات التقنية والفنية التي تمكن جهات تحقيق العدالة من القيام بالإجراءات التي تتناسب مع الطبيعة التقنية للأدلة الالكترونية، ومن ذلك إجراءات التحري والتفتيش والضبط بما يتناسب مع المكونات المعنوية للنظم المعلوماتية، وتوسيع صلاحيات تلك الجهات، إلى غير ذلك من الإجراءات التي تضمنها القانون الجزائري والاتفاقيات الدولية، وبما لا يتعارض مع المبادئ الخاصة باحترام حقوق الإنسان وخصوصياته.

3. إن القضايا التي عرضت على القضاء اليمني محدودة ولا تكاد تذكر، ونظراً لعدم وجود نصوص قانونية تتناسب مع تلك الجرائم، فإنهيتم تكييف تلك القضايا تكييفاً قانونياً يخالف الواقع خلافا لما ينبغي أن تكون عليه الحال، كأن تكيف قضية التلاعب بالبيانات المخزنة بنظام المعالجة الآلية للبيانات بهدف تحويل أموال بجريمة سرقة.
4. الجرائم المعلوماتية التي تناولها قانون العقوبات الجزائري، وكذلك النصوص التي تضمنها القانون الإجرائي والتعديلات التي ألحقت به، إضافة إلى نصوص القانون رقم (09- 04) المؤرخ في 5 غشت 2009، فذلك كله وإن اعتبر ميزة تستحق الإشادة في ظل قصور أغلب التشريعات العربية في هذا المجال، إلا أن الدراسة من جانب آخر قد بينت قصور التشريع الجزائري في عدم استكمال تجريم ما تبقى من جرائم معلوماتية ومنها:

- جرائم الاعتداء على نظام المعالجة الآلية للمعطيات بالإعاقة، أو الإفساد، وغيرها من الأفعال التي تستهدف تعطيل النظام عن العمل أو شل حركته كجريمة مستقلة، ولا يبرر ذلك بالاكتفاء بنصوص وردت في مواد أخرى، بعضها يجرم الاعتداءات العمدية على المعطيات الموجودة داخل النظام، وبعضها الآخر يجرمها كظرف مشدد على جريمة الدخول والبقاء، لأن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، إذ يلاحظ عدم سلامة ذلك التفسير، حيث أن المعطيات هي المستهدفة من الفعل وليس النظام، بالإضافة إلى أن المشرع الجزائري قد نص على الاعتداء غير العمدي على سير النظام كظرف مشدد لجريمة الدخول والبقاء، ولذا فإن الاعتداءات العمدية على سير النظام تفلت من العقاب.
- عدم النص على جرائم التزوير في مجال المعلوماتية، أو تعديل النصوص التقليدية المرتبطة بالتزوير مما يجعلها تتضمن التزوير المعلوماتي، حيث لا يمكن تطبيق النص الخاص بالتلاعب في البيانات عليها بما فيها تزوير المستند المعلوماتي، لأن البيانات المسجلة في الحاسوب تعد مخزنة بداخل النظام، أما المستند المعالج آلياً فقد يكون بداخل النظام وقد يكون بخارجه، وفي الحالتين يمكن أن يخضع للتزوير، ولذلك لا يمكن القول بخضوع المستند إذا كان خارج النظام للنصوص التقليدية لجريمة التزوير، وتطبيق النص المستحدث على تزوير المستندات أو البيانات المخزنة في النظام .
- عدم تضمن النصوص القانونية المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات الأفعال المستحدثة في ارتكاب الجريمة، والتي منها فعل التقاط المعلومات أو اعتراضها، باعتبارها أفعال تختلف عن الدخول والبقاء، مع أن المشرع الجزائري قد وضع في الجانب الإجرائي ما يمكن السلطات القائمة على تحقيق العدالة من التقاط المعطيات أو اعتراضها في حالات معينة، ولذا كان من باب أولى تجريم تلك الأفعال إذا تعلقت بارتكاب الجريمة.
- عدم تضمين النصوص القانونية ألفاظاً تدل على مواجهة ارتكاب الجرائم المعلوماتية التقليدية، فمع أنه بالإمكان تطبيق النصوص التقليدية عليها إلا أنه يفضل إضافة الألفاظ التي تدل عليها مثل جريمة غسيل الأموال والمخدرات والإرهاب، وغيرها

من الجرائم المرتكبة بواسطة الانترنت، فتلك الجرائم بحاجة إلى تشديد العقوبة عليها، بسب الخطورة التي ازدادت عن طريق ارتكابها بتلك التكنولوجيات. كما أنها قد وجدت بوجود الإنترنت أفعال تقنية لم تتضمنها النصوص التقليدية ومنها: إنشاء مواقع تهدف إلى ترويج المخدرات، ونشر معلومات على الشبكة لتعليم الطرق التي يتم بواسطتها تركيب مواد مخدرة باستخدام بعض الوصفات الطبية في الصيدليات، وغيرها من الأفعال ذات الطبيعة التقنية التي يمكن أن ترتكب بها جرائم المخدرات، و الإرهاب والتجسس، وغسيل الأموال وغيرها، مما يتطلب الأمر النص عليها.

- الجرائم المتعلقة بالإنترنت ومنها، جرائم الاعتداء على مواقع الانترنت، وجرائم الآداب المرتكبة بواسطة الحاسوب أو الإنترنت، بما فيها جرائم الاستغلال الجنسي للأطفال، وغيرها من الجرائم ذات الصلة بالتكنولوجيات الرقمية. فمع أن القانون الجزائري رقم(09-04) للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، قد تضمن في نطاق التطبيق الجرائم الماسة بأنظمة المعالجة الآلية للبيانات، وغيرها من الجرائم التي ترتكب بواسطة نظم الإعلام والاتصال إلا أن النص قد ورد عاماً ولم يتطرق لأية جريمة بذاتها.

5. إن الغرامات - المشار إليهاخصوصاً الغرامة التي يتحملها الشخص المعنوي في حال ارتكاب أيٍّ من الجرائم المعلوماتية - كبيرةجداً ، وقد تؤدي إلى إفلاس الشخصية المعنوية وإرهاقها مادياً ، وتؤثر على الشركاء المساهمين في الشخصية المعنوية، وخصوصا عندما ترتكب من الشخصية المعنوية ضد مؤسسات وهيئات القانون العام.

6. استخدم المشرع الجزائري لفظ المنظومة وليس النظام، مما يجعل القارئ للنص يستنتج أو يتبادر إلى ذهنه بأن النظام المحمي جنائياً وفقاً لنص المادة (394 مكرر)،لابد أن يكون عنصراً في منظومة لمعالجة البيانات، لكون لفظ المنظومة قد يشمل أكثر من نظام، مع أن الهدف من النص هو حماية الأنظمة المعلوماتية التي تعمل منفردة، أو تعمل ضمن منظومة معلوماتية، وكان الأولى أن يكون اللفظ في نص المادة بالنظام وليس المنظومة، لأن لفظ النظام يدخل فيه الدخول إلى نظام بمفرده أو إلى نظام يعمل ضمن منظومة معلوماتية.

7. تضمنت المادة (394 مكرر 2)من قانون العقوبات على عبارة "عمداً وعن طريق الغش" في جريمة التعامل مع المعطيات الناتجة أو التي يمكن أن يرتكب بها جريمة معلوماتية، مع أن باقي النصوص الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تضمنت عبارة " عن طريق الغش" فقط مما يوحي بأنها في هذا النص تدل على ضرورة توافر القصد الجنائي الخاص مع أن لفظ عن طريق الغش وعمداً تحمل معنى العمدية، فهي تؤكد العمدية وكان الأولى أن يكتفى بلفظ عن طريق الغش.

8. إن التشريع الجزائري قد تميز عن اليمني في الجانب الإجرائي من خلال تعديل قانون الإجراءات الجزائية في 2006، وصدور قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما في 2009، حيث تضمن الأول تمديد اختصاص ضباط الشرطة القضائية، وجهات التحقيق، والمحاكمة، على مستوى الإقليم الوطني إذا تطلب سير البحث والتحري أو التحقيق بالنسبة لعدد من الجرائم منها الجرائم المعلوماتية المنصوص عليها، بينما عالج مشكلة تتعدى الاختصاص المكاني إلى خارج الجزائر عندما يتطلب الأمر الرقابة أوتفتيش أنظمة معلوماتية موجودة خارج الدولة عن طريق التعاون والمساعدة القضائية بين الجزائر والدول التي ترتكب فيها أو منها الجريمة، أو تتحقق فيها النتيجة كلها أو بعضها، وكذلك أعفي تلك الجهات من التقيد ببعض الضمانات منها المتعلقة بمواعيد التفتيش، أو الأشخاص المطلوب حضورهم، كما تضمن الثاني النص على عديد من الإجراءات والالتزامات ذات الطابع التقني والتي من خلالها يستطيع ضابط الشرطة القضائية أو قاضي التحقيق الوقاية والتعامل مع تلك الجرائم ومرتكبيها، ومنها مراقبة الاتصالات الإلكترونية، والقواعد الإجرائية لتفتيش النظم المعلوماتية، وحجز المعطيات المعلوماتية، والالتزامات التي تقع على مقدمي الخدمات في مساعدة السلطات المكلفة بالتحريات القضائية، وكذلك الالتزامات الخاصة بمقدمي خدمة الإنترنت، كما تضمن القانون إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصالات ومكافحتها، وجعل

من ضمن مهامها القيام بأعمال الخبرة، وتبادل المعلومات مع نظيراتها في الخارج.

9. مع أن الاتفاقية الدولية لمكافحة الإجرام المعلوماتي، قد تضمنت مصطلحات جديدة تتناسب مع طبيعة الكيانات غير المادية التي يتم تفتيشها أو ضبطها، ومنها مصطلح الولوج، حيث يتناسب وطبيعة النظام والمعطيات والبرامج المدرجة فيه، مما يؤكد أن التفتيش على هذا النوع من المعطيات لابد وأن تتضمنها نصوص قانونية تكميلية، إلا أنه كان ينبغي أن يضاف إلى الولوج عبارة "بغرض التفتيش" وليس جعل الكلمة مرادفة للتفتيش، حيث أن لفظ الولوج منفرداً لا يعبر عن الغرض منه وهو التفتيش، فقد يقتصر الآمر على الولوج دون القيام بالتفتيش، وبذلك يكون المشرع الجزائري قد أحسن صنعاً عندما نص على الدخول بغرض التفتيش.

10. عدم تضمين المشرع الجزائري للاستثناء الخاص بوقت التفتيش، والأشخاص المطلوب حضورهم، ليشمل التفتيش على الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أسوة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، المنصوص عليها في القسم السابع من قانون العقوبات، حيث كان يجب على المشرع الجزائري طالما وقد وسع من صلاحيات سلطة الاستدلال والتحقيق حيال مكافحة هذه الجرائم من خلال القانون رقم (09-04) لسنة2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أن ينص على هذين الاستثناءين - بعدم تحديد وقت التفتيش- والأشخاص المطلوب حضورهم- على تلك الجرائم لاشتراكهما في العلة وهي الخطورة وسرعة إخفاء أدلتها.

11. إن أجهزت تحقيق العدالة مازالت - رغم تميزها عن كثير من الأجهزة في بعض البلدان العربية- بحاجة إلى التدريب الفني والتقني للتعامل مع الجرائم المعلوماتية، وتكيفها التكيف القانوني السليم، بخلاف مجرمي التقنية الرقمية الذين مافتئوا يتابعون كل جديد في مجال التكنولوجيا الرقمية ليطوروا من وسائلهم الإجرامية تبعاً لذلك.

12. عدم وصول التعاون الدولي في مجال مكافحة وضبط جرائم المعلوماتية إلى المستوى المطلوب، بسبب عدم وجود تشريعات في دول معينة لمواجهة هذه الجرائم، ووجودها في دول أخرى، كما أن ماهو مجرم في دولة معينة قد يعد عملا مباحاً في دولة أخرى.

ونتيجة لذلك يتعين إبداء الاقتراحات الآتية:

1. يجدر بالمشرع اليمني أن يتبنى تعديلات لقانون العقوبات رقم(12) لسنة 1994، وقانون الإجراءات رقم (13) لسنة 1994، ويضمنهما نصوصاً قانونية لمواجهة ومكافحة جرائم المعلوماتية، والاستفادة من التشريعات التي صدرت بهذا الشأن ومنها التشريعات الأجنبية، والعربية، بحيث يتلاشى أي قصور في تلك التشريعات، واضعاً في الاعتبار عدم إغفال الأتي:

- النص على جريمة السرقة المعلوماتية، وكذلك النصب وسائر جرائم الأموال، يوضح من خلاله طبيعة المال المعلوماتي وإدراجه ضمن الأموال القابلة للسرقة والنصب، وكذلك الأفعال التي يمكن أن يتم ارتكاب تلك الجرائم بواسطتها كالتقاط المعلومات أثناء تشغيل الجهاز، أو أثناء تبادل المعلومات وانتقالها من جهاز إلى آخر، أو يضيف عبارة بأي وسيلة أو بأي طريقة كانت.
- جريمة الدخول إلى نظام المعالجة الآلية للبيانات أو البقاء، بصورتها البسيطة والمشددة، وتشديد العقوبة في حال أن تستهدف تلك الأفعال المعطيات الحساسة والمخزنة بالأجهزة الحكومية، وعندما ترتكب من موظف.
- جريمة التلاعب العمدي بالبيانات المخزنة بالنظام بالمحو أو التعديل، أو الإدخال، وكذلك جريمة التعامل مع معطيات يتم من خلالها ارتكاب جريمة معلوماتية، أو تكون تلك المعطيات ناتجة عن جريمة معلوماتية، سواء عن طريق تصميم برامج فيروسية، أم عن طريق توفير أو نشر أو بحث عن تلك المعطيات أو غيرها من الأفعال التي تم الإشارة إليها.
- إعادة النظر في النصوص التقليدية في قانون العقوبات بما يتضمن تعديل وتشديد العقوبة على كل جريمة تزداد خطورتها ونسبة ارتكابها، إذا ماتم اقترافها بالوسائل الرقمية عن التقليدية، مثل التلاعب بالبيانات الرقمية الخاصة بالمرضى

في إحدى المستشفيات، والجرائم الماسة بالاقتصاد الوطني، والأمن القومي للدولة، وغيرها من الجرائم ذات الخطر العام .

- تجريم الشروع، والاتفاق الجنائي في جرائم المعلوماتية.
- النصوص الإجرائية التي من شأنها أن تعمل على تمديد الاختصاص المكاني في جرائم المعلوماتية، وتوسيع صلاحيات التحري والتفتيش والضبط، والخبرة، من خلال الإجراءات التقنية المستحدثة التي تسمح بالتفتيش ولو عن بعد، ووضع الترتيبات التقنية التي تسمح بالقيام بإجراءات التحري والتحقيق في مجال المعلوماتية، والاستعانة بكل من يستفاد منه في ذلك، وتحديد الالتزامات الخاصة بمقدمي خدمات الإنترنت، والتعاون الدولي، وغير ذلك من الإجراءات التي تضمنها القانون الجزائري والاتفاقيات والتوصيات الدولية.

2. يجدر بالمشرع الجزائري تلافي القصور الموجود في قانون المساس بأنظمة المعالجة الآلية للمعطيات، أوفي قانون الإجراءات الجنائية، أو في القانون رقم (09- 04) بشأن مكافحة جرائم العلوماتية، وتضمين نصوصه ألفاظاً صريحة تدل على الاعتراف بالمال ذي الطابع المعلوماتي أسوة بالمال المادي، وكذلك تلافي القصور في القوانين التي صدرت لمواجهة ومكافحة الإجرام المعلوماتي في التعديلات القادمة، ومن ذلك تجريم الأفعال التقنية التي يتم بها اعتراض المعطيات أو التقاطها من قبل الأشخاص أو الهيئات غير المخول لهم بذلك، وتضمين تلك الأفعال بجانب الأفعال التي تضمنتها القوانين.
3. النص على جريمة الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات في القانون اليمني والجزائري.
4. إعادة النظر في تخفيف عقوبة الغرامة للشخص المعنوي بالدرجة الأولى، وكذلك الطبيعي بما يتناسب مع تحقيق الهدف من إقرار العقوبة، وبما يتناسب مع الذمة المالية للأشخاص.
5. تجريم وتشديد العقوبات على الجرائم التي ترتكب بواسطة الشبكة المعلوماتية ومنها جرائم الاعتداء على الأعراض، والاستغلال الجنسي للأطفال، وجرائم غسيل الأموال والمخدرات، والإرهاب، وإضافة الألفاظ التي تدل على ارتكابها بواسطة النظم

المعلوماتية وشبكة الانترنت، وكذلك الأفعال التي يتم ارتكابها عن طريق الإنترنت، مثل إنشاء مواقع بهدف ارتكاب تلك الجرائم، أو الترويج لها.

6. يتعين على المشرع اليمني والجزائري وضع النصوص القانونية التي تحقق الحماية الجنائية لإساءة استخدام بطائق الائتمان .

7. الأحرى بالمشرع اليمني والجزائري الانضمام إلى أي تعاون دولي في مكافحة تلك الجرائم مع الحفاظ على كل ما يتعلق بالمصلحة الوطنية ومبدأ السيادة، وفي البداية تفعيل التعاون بين الدول العربية لمكافحة هذه الجرائم، وتسليم المجرمين كما فعلت الدول الأوروبية.

8. ضرورة قيام الجهات المعنية في كلا البلدين بتدريب الفئات العاملة في مجال تحقيق العدالة على التعامل مع تلك الجرائم بما يتناسب مع طبيعتها المنطقية، وتخصيص شرطة وقضاء متخصصان بالنظر في تلك الجرائم يكون لديهما الإلمام الكافي بالجوانب التقنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها، ونقترح إنشاء إدارة عامة في الجمهورية اليمنية لمكافحة جرائم الحاسوب تحدد مهامها على غرار الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال ومكافحتهما في الجزائر.

9. تبادل الخبرات بين دولتي اليمن والجزائر، فيما يخص التعاون في التدريب في مجال إعداد عناصر مؤهلة للتعامل مع تلك الجرائم.

10. تدريس مادة الإجرام في الإعلام الآلي في جوانبها الموضوعية والإجرائية لطلاب الليسانس في كلية الحقوق في كلا البلدين.

11. تدريس المادة نفسها في كلية الشرطة في كلا البلدين، وتدريب شرطة متخصصة يتم قبولها في كليات الشرطة، بحيث يشترط في المتقدمين إليه أن يكونوا حاصلين على مؤهل جامعي في علوم الحاسوب والشبكات.

إن تلك الجرائم والمشكلات المترتبة عليها تجعلنا نسعى لتشخيصها ومعرفة أسبابها، حتى نستطيع أن نقدم خدمة لأوطاننا في مكافحتها ومواجهتها بما يتفق وطبيعتها المعنوية، وموجاتها الكهرومغناطيسية، التي جعلت أسرارنا مكشوفة حتى ونحن مغلقين منازلنا على أنفسنا، فلم تعد الجدران والحواجز تفيد في منع الآخرين من الإطلاع على ما يجري ويدور في الأماكن المغلقة عبر جهاز الحاسوب والشبكة المعلوماتية.

قائمة المراجع

أولا: المراجع باللغة العربية

أ- معاجم اللغة العربية

- المعجم الوجيز، مجمع اللغة العربية، وزارة التربية والتعليم، جمهورية مصر العربية ط 1995.

ب- المراجع العامة والمتخصصة

- **الكتب العامة والمتخصصة**

1. إبراهيم حامد طنطاوي، أحكام التجريم والعقاب في قانون تنظيم الاتصالات المصري رقم(10) لسنة2003، دار النهضة العربية، القاهرة، 2003.
2. أحسن بوسقيعة، التحقيق القضائي على ضوء قانون 26 يونيو 2001، ط2، الديوان الوطني للأشغال التربوية، الجزائر، 2002.
3. أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديون الوطني للأشغال التربوية، الجزائر، 2002.
4. أحسن بوسقيعه، الوجيز في القانون الجزائي الخاص، ج1، ط5، دار هومه، الجزائر، 2006.
5. أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، ط1، الديوان الوطني للإشغال التربوية، 2000.
6. أحمد حسام طه تمام، الحماية الجنائية لتكنولوجيا الاتصالات، دار النهضة العربية، القاهرة، 2002.
7. أحمد المهدي، التحقيق الجنائي الابتدائي وضمانات المتهم المعلوماتي، دار العدالة للنشر والتوزيع، القاهرة، بدون تاريخ طبعة.
8. احمد خليفة الملط، الجرائم المعلوماتية، ،دار الفكر الجامعي، الإسكندرية، 2005.
9. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994.

10. آمال عبد الرحيم عثمان، شرح قانون العقوبات المصري، القسم الخاص، بدون ذكر دار النشر والبلد والتاريخ.
11. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط1، دار هومة للطباعة والنشر، الجزائر،2006.
12. أنطوان بطرس، موسوعة الكمبيوتر، ط2 ، مكتبة لبنان، 1994.
13. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقة الائتمان الممغنطة، دار النهضة العربية، القاهرة، 2003.
14. جميل عبد الباقي الصغير، المواجهة الجنائية لقرصنة البرامج التلفزيونية المدفوعة الأجر، دار النهضة العربية، القاهرة، 2002.
15. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.
16. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي –الأحكام الموضوعية لجرائم الانترنت، دار النهضة العربية، القاهرة، 2002 .
17. حسن علي مجلي، جرائم الاعتداء على الملكية في القانون والقضاء اليمني، ط1، عالم الكتب اليمنية، صنعاء،2007 .
18. حسن علي مجلي، المحاكمة في قانون الإجراءات الجزائية اليمني، بدون ذكر دار النشر ورقم الطبعة، 2001.
19. حسني الجندي ، مجدي عقلان ، شرح قانون العقوبات اليمني، بدون ذكر دار النشر والتاريخ.
20. حسني الجندي، شرح قانون الإجراءات الجزائية اليمني، بدون دار النشر، بدون رقم الطبعة،1990.
21. سامح محمد عبد الحكم، الحماية الجنائية لبطاقات الائتمان، دار النهضة العربية، القاهرة، 2003.
22. سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، المؤسسة الجامعية، الإسكندرية، 1979.

23. خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية المصري، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
24. سامي حامد عباد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، ط1، دار الفكر الجامعي الإسكندرية،2007.
25. سعد غالب ياسين، بشير عباس العلاق، الأعمال الإلكترونية، دار المناهج، عمان- الأردن، 2006.
26. سمير عاليه، شرح قانون العقوبات - القسم العام- دراسة مقارنه، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، بدون ذكر السنة.
27. ظاهري حسن، الوجيز في شرح قانون الإجراءات الجزائية، ط2، دار المحمدية العامة، الجزائر،1999.
28. عبد الحميد ألشواربي، إذن التفتيش في ضوء القضاء والفقه، منشأة المعارف، الإسكندرية، بدون تاريخ طبعة.
29. عبد الفتاح بيومي حجازي، الأحداث والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2002.
30. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2004.
31. عبد الفتاح سليمان، مكافحة غسل الأموال، دار الكتب القانونية، القاهرة، 2005.
32. عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، بدون رقم الطبعة، ودار النشر، والتاريخ.
33. عبد الفتاح مصطفى الصيفي، قانون العقوبات -النظرية العامة، دار الهدى، الإسكندرية، بدون ذكر السنة.
34. عبد الله احمد فروان، أحكام السرقة بالتسبب في الشريعة والقانون، ط1، مكتبة الفاروق صنعاء، 2005/2004.
35. عبد الله أوهايبية، شرح قانون الإجراءات الجزائري، دار هومه للطباعة والنشر، الجزائر، 2005.

36. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط3، دار النهضة العربية، القاهرة، 2004.
37. عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة، الإسكندرية، 2008.
38. عفيفي كامل عفيفي ،جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط2، بدون ذكر دار النشر،2000 .
39. على حسن الشامي، جريمة الاتفاق الجنائي في قانون العقوبات المصري، مطبعة لجنة التأليف والترجمة والنشر، القاهرة، 1999.
40. علي حسن الشرفي، شرح الأحكام العامة للتشريع العقابي اليمني وفقا لمشروع القانون الشرعي للجرائم والعقوبات، دار المنار، القاهرة،1993.
41. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999.
42. عمر سالم، الحماية الجنائية لبطاقة الوفاء، ط1، دار النهضة العربية، القاهرة، 1995.
43. عمر عيسى ألفقي، الجرائم المعلوماتية، دار الكتب الجامعي الحديث، الإسكندرية، 2006.
44. عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها(المراقبة الدولية للسياسة الجنائية) ملخص الترجمة العربية لمرشد الأمم المتحدة1999، ط1، دار النهضة العربية، القاهرة، 2005.
45. عمر محمد ين يونس، يوسف أمين شاكير، غسل الأموال عبر الانترنت وموقف السياسة الجنائية، ط1، دار النهضة العربية، 2004.
46. فضل العيش، قانون العقوبات الجزائري، وفقا للتعديلات الأخيرة 2006، منشورات بغدادي، الجزائر،2007.
47. محمد أبو العلاء عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد، دار الفكر العربي، القاهرة، 1997.

48. محمد أحمد المخلافي، العولمة والملكية الفكرية، ط1، مؤسسة العفيف الثقافية، صنعاء، اليمن، 2002.
49. محمد الصيرفي، الإدارة الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2006.
50. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.
51. محمد راجح نجاد، شرح قانون الإجراءات الجزائية اليمني، ط1، بدون دار نشر،2000.
52. محمد سامي الشواء، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية ،القاهرة.
53. محمد سامي الشواء، الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية، 1998.
54. محمد صبحي نجم، شرح قانون العقوبات الجزائري –القسم الخاص ،ط5، ديوان المطبوعات الجامعية،2004.
55. محمد على العريان ، انعكاس ثورة المعلومات على قانون العقوبات، دار الجامعة للنشر، الإسكندرية، 2004.
56. محمد عبد الظاهر حسين، المسئولية القانونية في مجال شبكة الإنترنت، المؤسسة الفنية للطباعة والنشر، 2004.
57. محمد حسن قاسم، مراحل التفاوض في عقد الملكية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، بدون ذكر سنة النشر.
58. محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسوب الآلي والانترنت، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
59. محند شريف بلعيد، هندسة ووظائف الكمبيوتر، بدون رقم الطبعة، الصفحات الزرقاء، الجزائر،2001.
60. محي الدين عكاشة، حقوق المؤلف على ضوء القانون الجزائري الجديد، ط2، ديوان المطبوعات الجامعية، الجزائر2007.

61. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، 2001.
62. مروك نصر الدين، محاضرات في الإثبات الجنائي، ج2، دار هومة، الجزائر، 2004.
63. مصطفى مجدي هرجه، جرائم المخدرات في ضوء الفقه والقضاء، دار المطبوعات الجامعية، الإسكندرية،1992.
64. مصطفى محمد موسى ، أساليب إجرامية بالتقنية الرقمية، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة،2003.
65. مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة،2001.
66. مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، ط1، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2003.
67. منير الجنبيهي ومحمود الجنبيهي، بروتوكولات وقوانين الإنترنت، دار الفكر الجامعي الإسكندرية، بدون رقم وتاريخ الطبعة.
68. منير محمد الجنبيهى ، ممدوح محمد الجنبيهى، امن المعلومات الالكترونية، دار الفكر الجامعي، الإسكندرية،2005.
69. منير محمد الجنبيهي ومحمود محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي، الإسكندرية، 2004.
70. موريس صادق، المشكلات العملية في الجرائم الجنائية، دار الكتب القانونية، بيروت، 2000.
71. نعيم مغبغب، مخاطر المعلومات والانترنت- المخاطر على الحياة الخاصة- دراسة في القانون المقارن،1998، بدون ذكر البلد ودار النشر.
72. هدى حامد قشقوش، جرائم الحاسوب الالكتروني في التشريع المقارن، دار النهضة العربية القاهرة ،1992.
73. نزيه نعيم شلال، دعاوي الاحتيال وما جرى مجراه، المؤسسة الحديثة للكتاب، طرابلس- لبنان، بدون ذكر سنة النشر.

74. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، ط1، مكتبة الآلات الحديثة، أسيوط، 1992.
75. هلالي عبد أللاه احمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، ط1، دار النهضة العربية، القاهرة،2003.
76. هلالي عبد أللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، النسر الذهبي للطباعة ، القاهرة،1999.
77. هلالي عبد أللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي، القاهرة،2002.
78. ياسر الصاوي إدارة المعرفة وتكنولوجيا المعلومات، ط1، دار السحاب، القاهرة، 2007.
79. يوسف دلاندة، قانون العقوبات منقح بالتعديلات التي أدخلت عليه بموجب القانون رقم(04- 15) المؤرخ في 10 نوفمبر 2004 ومدعم بأحدث مبادئ واجتهادات المحكمة العليا، دار هومه، الجزائر، 2005.

- **الرسائل العلمية (دكتوراه وماجستير)**

1. احمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، رسالة دكتوراه في القانون الجنائي دراسة مقارنه، دار النهضة العربية، القاهرة، 2000.
2. أيمن عبد الحفيظ عبد الحميد سليمان: إستراتيجية مكافحة الجرائم ألناشئه عن استخدام الحاسوب الآلي دراسة مقارنه، رسالة دكتوراه في علوم الشرطة، أكاديمية الشرطة، القاهرة، 2003.
3. عبد الغني محمد عطا الله: الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، 2005 .
4. علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا،ط1، عالم الكتاب الحديث ،اربد – الأردن،2004.

5. علي يوسف حربه: النتيجة الإجرامية دراسة مقارنه، رسالة دكتوراه، جامعة القاهرة، 1998.
6. عمر محمد أبو بكر يونس: الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة القاهرة، دار النهضة العربية، 2004 .
7. محمد راجح نجاد: حقوق المتهم في مرحلة جمع الاستدلال، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، دار المنار، القاهرة،1994.
8. نائلة عادل محمد فريد قورة: جرائم الحاسوب الآلي الاقتصادية ، رسالة دكتوراه، كلية الحقوق-جامعة حلوان، ط1، 2005، منشورات الحلبي الحقوقية، بيروت،ص162.
9. آمال قارة: الجريمة المعلوماتية، رسالة ماجستير قدمت إلى كلية الحقوق، بن عكنون، جامعة الجزائر، 2004.
10. خلف الله عبد العزيز: جريمة تبييض الأموال، رسالة ماجستير، كلية الحقوق والعلوم الإدارية بن عكنون، 2004.
11. سعيد حميدة: الشروع أو المحاولة في قانون العقوبات الجزائري، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 1979.ص75.
12. سليم مرحالي: مفهوم الإرهاب في القانون الدولي، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر، 2002/2001.
13. شروقي محترف: التفتيش في قانون الإجراءات الجزائية الجزائري، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، 2005- 2008.
14. فهد سلطان محمد احمد بن سليمان: مواجهة جرائم الانترنت دراسة مقارنه، رسالة ماجستير في القانون الجنائي، جامعة القاهرة، كلية الحقوق ،2004.
15. محمد أمين احمد الشوابكة: الجريمة المعلوماتية ، رسالة ماجستير، جامعة القاهرة، دار الثقافة للنشر والتوزيع، عمان، ط1 2004.
16. محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة ماجستير، دار الجامعة الجديدة، الإسكندرية، 2007.

17. محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع الشبكة الانترنت، رسالة ماجستير، كلية الحقوق ، جامعة القاهرة، 2004.
18. محمود احمد عباينة: جرائم الحاسوب وأبعادها الدولية ، رسالة ماجستير، الجامعة الأردنية، دار الثقافة ، عمان-الأردن،2005.
19. محمد أمين أحمد الشوابكة: الجريمة المعلوماتية، رسالة ماجستير، جامعة القاهرة، ط1، دار الثقافة للنشر والتوزيع، عمان، 2004.
20. نبيله هبه هروال: الجوانب الإجرائية لجرائم الإنترنت، رسالة ماجستير، ط1،دار الفكر الجامعي، الإسكندرية ،2007.
21. نهلا عبد القادر المومني: الجرائم المعلوماتية، رسالة ماجستير، الجامعة الأردنية، ط1، دار الثقافة للنشر،عمان الأردن،2007.

ج- المراجع الخاصة

- **البحوث والمقالات**

1. إبراهيم احمد إبراهيم، الحماية الدولية لبرامج الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر، الإمارات العربية المتحدة، 2000.
2. أبو بكر الزهيري، مخاطر غسل الأموال على الاقتصاد الوطني، ورقة عمل مقدمة إلى ندوة غسل الأموال ومخاطرة، صنعاء، اليمن، 2008/11/18.
3. أحمد عبد الكريم سلامة، الإنترنت والقانون الدولي الخاص فراق أم تلاق، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من1-3مايو 2000، المجلد الثاني ،ط3، 2000.
4. سعود بن عبد العزيز المريشد، غسل الأموال الإلكتروني وفقا للنظام السعودي والنظام المقارن والمعايير الدولية، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني، الذي تم تنظيمه من قبل رأسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر 2007.

5. عائض بن فائز الشهري، صالح بن يحيى القحطاني، دور تقنية المعلومات في تعزيز الأمن الوطني وطرق حمايتها، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني الذي تم تنظيمه من قبل رأسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر 2007.
6. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة،1-3 مايو2000.
7. عمر الفاروق الحسيني، جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000 .
8. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 1- 3 مايو 2000م، ج2، ط3.
9. محمد أبو العلا عقيده، مواجهة الجرائم الناشئة عن استخدام الحاسب الآلي، بحث مقدم إلى مؤتمر حول الكمبيوتر والقانون- ضفاف بحيرة قارون بالفيوم، من 29يناير الى 1 فبراير 1994.
10. محمد بن حاج الطاهر وعبد القادر دوحة، التحديات الأمنية والقضائية لمنع الجريمة الإلكترونية، بحث مقدم إلى الملتقى الوطني الأول- القانون وقضايا الساعة- النظام القانوني للمجتمع الالكتروني، المركز الجامعي، خميس مليانة، ولاية عين الدفلى، الجزائر، من9- 11 مارس 2008.
11. مصطفى فواد عبيد، التنقيب في قواعد البيانات واستكشاف المعلومات المخبأة فيها، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني، المملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر 2007، مجلد 2، ص1277.

12. *تيطاوني الحاج*، الانترنت عملاق المعلوماتية، بحث مقدم إلى الملتقى الوطني الأول، القانون وقضايا الساعة- النظام القانوني للمجتمع الالكتروني، المركز الجامعي بخميس مليانة، ولاية عين الدفلى، الجزائر، من9- 11 مارس 2008. ع 4، سبتمبر 2009.
13. نائل صالح عبد الرحمن، واقع جرائم الحاسوب الآلي في التشريع الجزائي الأردني، ورقة عمل مقدمة إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة،2000.
14. هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الالكتروني، ج 2، بحث قُدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الحقوق، جامعة الإمارات العربية المتحدة، 2000.
15. هشام محمد فريد رستم، أصول التحقيق الجنائي الفني في جرائم الحاسوب، بحث مقدم إلى مؤتمر القانون والكمبيوتر، الإمارات العربية المتحدة. من1-3مايو 2000.
16. هند بنت سليمان الخليفة، الحاسب الجنائي في الدول الغربية دورة استطلاعية، بحث مقدم إلى مؤتمر تقنية المعلومات والأمن الوطني، الذي تم تنظيمه من قبل رأسة هيئة الاستخبارات العامة بالمملكة العربية السعودية- الرياض، من 1 إلى 4 ديسمبر،2007.

- **الدوريات**

1. أحسن مظفر الرزو، ((الأمن ألمعلوماتي معالجة قانونية أولية))، مجلة الأمن والقانون، صادرة عن أكاديمية شرطة دبي، الإمارات العربية المتحدة، ع1، س12، يناير 2004.
2. زياد على عربية، ((غسيل الأموال)) مجلة الأمن والقانون، صادرة عن أكاديمية الشرطة بدبي، ع1، يناير2004.
3. عادل الطبطبائي، ((جرائم ذوي الياقات البيضاء))، مجلة الحقوق الكويتية، فصلية علمية محكمة، ع3، س23، سبتمبر 1999.

4. عبد العزيز العشاوي، ((الجرائم المنظمة بين الجريمة الوطنية والجريمة الدولية))، مجلة كلية أصول الدين للبحوث والدراسات الإسلامية، ع3، سبتمبر2000.
5. الغوثي بن ملحه، ((الجريمة المنظمة في قانون العقوبات الجزائري))، مجلة كلية أصول الدين للبحوث والدراسات الإسلامية، ع3، سبتمبر2000.
6. عبد التواب معوض، ((لاتفاق الجنائي العام في ضوء الحكم بعدم دستورية المادة 48 عقوبات مصري)) المجلة القانونية الاقتصادية، جامعة الزقازيق، كلية الحقوق، العدد17،2005.
7. علي محمد الانسي، ((التأثيرات المختلفة على الأمن القومي اليمني))، مجلة الأكاديمية العسكرية العليا، سنوية،ع 4، سبتمبر 2009.
8. محمد حافظ رهوان، ((عملية غسيل الأموال، مفهومها، خطورتها وإستراتيجية مكافحتها)) مجلة الأمن والقانون، أكاديمية شرطة دبي، ع2، يوليو 2002.
9. محمد الأمين البشيري ((التحقيق في جرائم الحاسب الآلي والإنترنت)) المجلة العربية للدراسات الأمنية والتدريب، صادرة عن أكاديمية نايف للعلوم الأمنية، الرياض، ع30، نوفمبر2000.
10. محمد سعيد مرهود ((جرائم ذوي الياقات البيضاء))، مجلة الحقوق الكويتية، فصلية علمية محكمة، ع3، س23، سبتمبر 1999.
11. محافظي محمود، ((عصر العولمة واستعمال الإنترنت في اختلاس الأموال))، مجلة دراسات قانونية، دار القبة للنشر والتوزيع، الجزائر ع(5)، ديسمبر 2002.
12. نائل علي مساعد، ((أركان الفعل الضار في القانون الأردني))، مجله دراسات، علمية محكمة صادرة عن عمادة البحث العلمي بالجامعة الأردنية، ع(1)، مايو 2005.
13. نصرون وردية، ((جريمة الغش في الإعلام الآلي)) المجلة القضائية ،المحكمة العليا ، الجزائر،2002.
14. مجلة تكنولوجيا الاتصالات والمعلومات، صادرة عن وزارة الاتصالات وتقنية المعلومات اليمنية، ع42، ديسمبر 2003.
15. مجلة تكنولوجيا الاتصالات والمعلومات، ع44، فبراير 2005.

16. مجلة الفيصل، شهرية، صادرة عن مركز الملك فيصل للبحوث الدراسات الإسلامية، السعودية، ع371، مايو 2007.

- **الوثائق والمعاهدات والقوانين والأحكام**

- **الوثائق**

1. دستور الجمهورية اليمنية .
2. الدستور الجزائري.

- **المعاهدات**

1. اتفاقية بودابست 2001 بشأن مكافحة الإجرام المعلوماتي.
2. اتفاقية جنيف 1937 بشان التعاون في مكافحة الإرهاب.
3. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية،2000.

- **القوانين**

1. القانون المدني اليمني رقم (14)لسنة 2002.
2. قانون العقوبات رقم (12)لسنة 1994 (ج.ر. ع 3/19لسنة 1994.
3. قانون الإجراءات الجزائية رقم 13 لسنة 1994(ج.ر19ج4 لسنة1994).
4. القانون رقم (3) لسنة 1993 بشأن مكافحة الإتجار والاستعمال غير المشروعين للمخدرات والمؤثرات العقلية.
5. القانون رقم (35) لسنة 2003 بشأن مكافحة غسيل الأموال.
6. القانون رقم (19)لسنة 1994 بشأن الحق الفكري، الجريدة الرسمية، العدد20،31 أكتوبر 1994.
7. الأمر رقم (75 - 58) المؤرخ في 26 سبتمبر سنة 1975يتضمن القانون المدني الجزائري المعدل بعدد من الأوامر والقوانين أخرها القانون رقم (07-05) المؤرخ في 13 مايو 2007.
8. الأمر رقم(66- 156) المؤرخ في 8 يونيو 1966يتضمن قانون العقوبات الجزائري المُعَدَل والمُتَمَم بعدد من الأوامر والقوانين أخرها القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006 (ج.ر 84، 24 ديسمبر 2006).

9. قانون العقوبات الجزائري رقم (04- 15) المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات.
10. الأمر رقم (66-156) المؤرخ في 8 يونيو 1966يتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم بعدد من الأوامر والقوانين أخرها القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006.
11. القانون رقم (09- 04) المؤرخ في 2009/8/5 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الصادرة بتاريخ 2009/8/16،ع 47.
12. القانون رقم (05-1)المؤرخ في 27ذي الحجة عام 1425الموافق 6 فبراير سنة 2005 بشأن الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهم.
13. القانون رقم (04-18) المؤرخ في 25 ديسمبر سنة 2004، يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين، ط1، الديوان الوطني للأشغال التربوية، الجزائر، 2005.
14. الأمر رقم 05/03 المؤرخ في 2003/7/19 المتعلق بحق المؤلف والحقوق المجاورة
15. قانون العقوبات القطري رقم (11) لسنة 2004 .
16. المرسوم السلطاني العماني رقم(72/ 2001) بشأن تعديل بعض أحكام قانون الجزاء العماني رقم (74/7)، الجريدة الرسمية رقم (698) الصادرة في 2001/7/1.
17. نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم(م/17) المؤرخ في8/ 3/ 1428 هـ، الموافق 26/ 3/ 2007 بناء على قرار مجلس الوزراء رقم (79) المؤرخ في 1428/3/7هـ .
18. القرار الوزاري المؤرخ في 14 ابريل 2007 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي.(ج.ر 36 ، 3يونيو 2007، من ص 14 –ص17)

- **الأحكام غير المنشورة:**

19. حكم المحكمة الجزائية اليمنية المتخصصة الابتدائية رقم (7) في القضية الجزائية رقم (29) بتاريخ 2005/5/14.
20. حكم المحكمة الجزائية الأستنافية اليمنية المتخصصة رقم (27) في القضية الجزائية رقم (13) بتاريخ 2005/9/20.

ثانيا: المراجع باللغة الأجنبية:

1. Bouder Hadjira, Quelle protection pour les programmes d'ordinateur en droit Algérien? Revue algérienne des sciences juridiques économiques et politiquesfacilté de droit de ben aknoun -Alger, volume'&n°02/2004,p94 et après
2. Said Bachir, criminalité informatique en Algérie, état des lieux et perspectives, Mémoire Master université de Lausanne, suisse, 2009.
3. Solange Ghernaouti –Hélie, <<Sécurité Informatique et réseaux,>> du mod, paris, 2006.
4. Boudoumi Abderrahmane: Internet et droit pénal, intervention colloque <<l'espace électronique et le droit >> 9 et 11Mars2008.
5. Jean-Wilfried noël, <<internet et enquête judiciaire>>, Le droit international de l'internet; Bruylant,2002.
6. Guy De Vel, <<La convention sur la cybercriminalité>>, Le droit international de l'internet, Bruylant, Bruxelles,2002,p.238.
7. Cyber terrorism –Testimony before the U.S. House of Representatives By :Dr. Dorothy E. Denning / Georgetown Uni. May 23 ,2000 . Available on line in 4/10/2009.
8. Jacques Plays: Internet et enquête judiciaire, étude présenté au colloque organisé à Paris les 19 et 20 novembre 2001 par le Ministère de la justice, L'Université Paris I Panthéon Sorbonne et l'Association Arpeje. Sur le droit international de l'internet Sous la direction de Georges Chatillon Bruyant Bruxelles 2002.
9. Aoughlis Samir, <<Identification Automatique de Personnes à partir de l'Iris de l'œil et de l'Empreinte Digitale >> Mémoire de Magister, Université Mouloud Mammeri, Tizi- Ouzou, Algérie, 2007.
10. DIDIER Gobert et Étienne Montero: La signature dans les contrats et les paiements électroniques, cahiers du centre de recherches informatique et droit, Bruylant. Bruxelles. 2000 .

ثالثا: مراجع شبكة المعلومات الدولية (الإنترنت):

- **مواقع باللغة العربية**

- بحوث ومقالات وورق عمل

1. احمد حسن، جرائم غسيل الأموال في التشريع العراقي، بحث منشور على الشبكة المعلوماتية متاح في تاريخ 10/ 2009/7 على الرابط:

http://www.iraqja.org/judicalsheet3/research/gasil_amwal_raaed.htm

2. أمين عباس، الجريمة الإلكترونية والقانون في اليمن، موقع وكالة الأنباء اليمنية سبا، ت.د 2008/3/19 على الرابط:

http://www.sabanews.net/ar/news142248.htm

3. حسن عزيز نور الحلو: لإرهاب في القانون الدولي، رسالة ماجستير، الأكاديمية العربية المفتوحة - الدانمرك، 2007، متاحة على موقع منتدى كلية الحقوق- جامعة المنصورة، ت.د 2006/6/10.

http://www.f-law.net/law/showthread.php?t=6420

4. حسين بن سعيد الغافري، الإنترنت وآفة المخدرات، ورقة عمل قدمت لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت الذي انعقد بالقاهرة من 2 إلى4 يونيو2008، منشور على موقع منتدى كلية الحقوق- جامعة المنصورة، ت.د 2009/4/20، على الرابط:

http://www.f-law.net/law/showthread.php?t=28534

5. حسين بن سعيد سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، بحث منشور على شبكة الإنترنت، موقع المنشاوي، ت.د 2009/4/5 على الرابط.

www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014

6. خالد الطويل، الجريمة الإلكترونية، مقال منشور على موقع شبكة روايات، ت.د 2009/8/16 على الرابط:

http://www.rewayatnet.net/forum/archive/index.php/t-4004.htm

7. دانيال لاركين، محاربة جرائم الإنترنت، مقال في شبكة الإنترنت على موقع America -.gov ، ت.د 2009/1/13، على الرابط:

http://www.america.gov/st/democracy-arabic/2008/May/20081117124454snmassabla0.2601086.html

8. سامي الحربي، الإرهاب الالكتروني هل هو حقيقة أم خيال، جريدة الرياض، ع - 13449، الأربعاء 11 ربيع الأول 1426هـ الموافق20 إبريل 2005م، وتم التأكد من أن المعلومات مازالت متاحة على الشبكة في 2009/10/4 على الرابط:

http://www.alriyadh.com/2005/04/20/article57983.html

9. سعيد عبد الخالق، القانون المصري رقم 80 لسنة 2002 الخاص بمكافحة غسل الأموال فلسفته واهم ملامحه، موقع البوابة القانونية، ت.د 2008/6/13،على الرابط :
http://www.tashreaat.com/view_studies2.asp?std_id=26
10. سلطان محيا الديحاني، التحري في الجريمة المعلوماتية، جريدة القبس الكويتية،ع30،12392 نوفمبر2007، ت.د 2008/1/20 على الرابط:
http://www.alqabas.com.kw/Final/NewspaperWebsite/NewspaperPublic/ArticlePage.aspx?ArticleID=230005
11. شيماء عبد الغني محمد عطاء الله، مكافحة الجرائم المعلوماتية وفقا لنظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، بحث منشور على موقع منتدى كلية الحقوق – جامعة المنصورة، ت.د 2009/8/9 على الرباط:
http://www.f-law.net/law/showthread.php?t=28512
12. وليد عكوم ،التحقيق في جرائم الحاسوب، مقال منشور على موقع كلية الحقوق – جامعة المنصورة، تم التأكد من أن المقال مازال متاح في الموقع بتاريخ2009/6/7 على الرابط:
http://www.f-law.net/law/showthread.php?t=11336
13. عاصم عبد الجبار سعــد، الإثبات في قانون المعاملات الإلكترونية العماني رقم(69)لسنة 2008، و قانون الإثبات في المعاملات المدنية والتجارية العماني رقم (86) لعام 2008، س .د 6 BM ت.د 2008/4/9 على الرابط:
http://www.ita.gov.om/ITAPortal_AR/Data/ImgGallery/FID200812383916827/%D8%A7%D9%84%D8%A5%D8%AB%D8%A8%D8%A7%D8%AA%20%D9%81%D9%8A%20%D8%A7%D9%84%D8%B9%D9%82%D8%AF%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%20%D8%AA%D8%B9%D8%AF%D9%8A%D9%84%20.doc
14. عايض ألمري، أمن المعلومات- ماهيتها وعناصرها وإستراتيجيتها، بحث منشور على موقع الدكتور المري، ت.د 2008/6/11على الرابط:
http://www.dralmarri.com/show.asp?field=res_a&id=205
15. عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008، منشور على موقع منتدى كلية الحقوق- جامعة المنصورة، ت.د 2009/4/10 على الرابط:
http://www.f-law.net/law/showthread.php?t=28535
16. عبد المؤمن شجاع، جريمة التحويل الإلكتروني غير المشروع للأموال، مقال منشور على موقع المحكمة التجارية اليمنية، ت.د 2008/3/19 على الرابط:
http://www.qada.gov.ye/garymah.asp

17. عبدا لله علي حسين محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، مقال منشور على شبكة الإنترنت، موقع منتدى كلية الحقوق- جامعة المنصورة ، على الرابط :

http//www.f-law.net/law/showthread.php?t=1312

18. علي سليمان، مقال منشور على موقع المحكمة التجارية اليمنية، ت.د 2008/3/19 على الرابط:

http://www.qada.gov.ye/garymah.asp

19. علي محمود حمود: الأدلة الإلكترونية المتحصلة من الإثبات الإلكتروني في ظل الإثبات الجنائي، بحث تم تقديمه إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، من 26 – 28 نيسان 2003، منشور على موقع كلية الحقوق جامعة المنصورة،س.د 11 bm ،ت.د 2009/4/8،على الرابط:

Http://www.f-law.net/law/shozthread.php?t=1133

20. فيل وليامز، الجريمة المنظمة وجرائم الشبكات الإلكترونية، دراسة متاحة على موقع منتدى هيئة الادعاء العام بالمملكة العربية السعودية، ت. د 2009/3/8، على الرابط:

http://vb.bip.gov.sa/showthread.php?t=5202

21. اللواء صلاح الدين سليم - خبير بأكاديمية ناصر العسكرية، مصر، صحيفة الإخبارية الالكترونية، 2006-05-05، تم التأكد من أن الموضوع مازال منشور في 30/ 2009/9:على الرابط

http://www.sharesgate.com/vb/t5856.html

22. محمد أبو العلا عقيده، التحقيق وجمع الأدلة في مجال الجريمة الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر، أكاديمية شرطة دبي، من 26 نيسان 2003 : 28 نيسان 2003 ، ت.د 2009/1/30، موقع عرب قانون، وموقع مندى كلية الحقوق – جامعة المنصورة على الرابطين:

http://www.arblaws.com/board/archive/index.php/t-2275.html
http://www.f-law.net/law/showthread.php?t=2208

23. محمد عادل، إجراءات جمع الأدلة في شبكة المعلومات، موقع كلية الحقوق جامعة المنصورة، ت.د 5/18/ 2009على الرابط:

http://www.f-law.net/law/showthread.php?t=1312

24. محمد عبد الله المنشاوي، الانترنت بدايته وتعريفه واهم جرائمه، أكاديمية نايف للعلوم الأمنية، المملكة العربية ألسعوديه، ت.د 30/ 6/ 2010على الرابط:

law.htm20%the20%http://www.minshawi.com/old/internetcrim-in

25. محمد عبدا لله المنشاوي، المخاطر الأمنية للإنترنت، بحث منشور على موقع المنشاوي للدراسات والبحوث، ت.د 2009/9/1، على الرابط:
http://www.minshawi.com/old/internet-crime.htm

26. محمد محمد الألفي ، مكافحة جرائم الإرهاب عبر الشبكة، موقع شبكة النباء المعلوماتية، ت.د 2006/7/6،على الرابط:
http://www.annabaa.org/nbanews/55/297.htm

27. محمد محمد الألفي، جرائم التجسس والإرهاب الالكتروني عبر الإنترنت، مقال منشور على موقع شبكة النبأ المعلوماتية، الأربعاء 22/شباط(فبراير)/2006، ت.د 2007/3/5، وكذلك في جريدة 26 سبتمبر اليمنية، الاثنين، 16 يناير، 2006،على الرابطين:
http://www.annabaa.org/nbanews/54/273.htm
http://www.annabaa.org/nbanews/54/273.htm

28. محمود صالح العادلي، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية، بحث منشور في منتدى قوانين قطر، وملف ورد على الموقع التالي ، وكذلك موقع منتدى الشروق أو لاين تم التأكد من أن البحث مازال منشور في 2009/10/10 علي الروابط:
http://www.law-zag.com/vb/showthread.php?s=db2dfbed90fe7d5cb217bee924b47901&p=33245#post33245
http://www.ituarabic.org/coe/2006/E-Crime/Documents%20and%20Presentations/DAY%201/Doc7-Om.PPT
http://www.echoroukonline.com/montada/showthread.php?t=7916

29. مراد رشدي، غسل الأموال عبر الوسائل الإلكترونية، بحث قدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، الإمارات العربية المتحدة، من 26 /2003/4 إلى 2003/4/28، منشور على موقع منتدى هيئة التحقيق والادعاء بالمملكة العربية السعودية، ت.د 2006/1/8
http://vb.bip.gov.sa/archive/index.php?t-6909.html

30. ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (IP/TCP) في بحث و تحقيق جرائم الحاسوب، منتدى كلية الحقوق- جامعة المنصورة، ت.د 2009/6/25، على الرابط:
http://www.f-law.net/law/showthread.php?p=79241

31. موساي معمر، الإثبات الإلكتروني في القانون، منتدى الجزائرية للقانون والحقوق، ت.د 2009/4/9.على الرابط:
http://forum.law-dz.com/index.php?showtopic=2661

32. موسى مسعود أرحومة، الإرهاب والانترنت، بحث مقدم إلى المؤتمر الدولي بجامعة الحسين بن طلال، الأردن، حول الإرهاب في العصر الرقمي، ت.د 10/ 3/ 2007، منشور على شبكة المعلومات الدولية،على الربط:
http://www.ipcciraq.org/alhallmg/print.php?id=274
37- وليد عكوم، التحقيق في جرائم الحاسوب، مقال منشور على موقع الدليل الإلكتروني للقانون العربي، وموقع منتدى كلية الحقوق – جامعة المنصورة، ت.د 2006/12/20 ، و2008/7/3على الرابطين:
http://www.arablawinfo.com/Researches_AR/126.doc
http://www.f-law.net/law/showthread.php?t=11336
38- يونس عرب حجية الإثبات بالمستخرجات الإلكترونية في الأعمال المصرفية، مقال منشور في منتدى كلية الحقوق- جامعة المنصورة، س .د 6 BM ت.د 2008/4/9 على الرابط
http://www.f-law.net/law/showthread.php?p=156142
39- يونس عرب: تطور التشريعات في مجال مكافحة الجرائم المعلوماتية، ورقة عمل قدمت إلى ورشة العمل التي تبنتها هيئة تنظيم الاتصالات بسلطنة عمان،2-4 2006 ، ت.د 10/ 2008/2منشوره على شبكة المعلومات الدولية على الربط:
http://www.ituarabic.org/coe/2006/E-Crime/Documents%20and%20Presentations/DAY%201/Doc6-Jor.DOC
40- يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل تم تقديمها إلى مؤتمر الأمن العربي، أبو ظبي، 2002/2/12، منشورة على شبكة الإنترنت، ت.د 2009/1/30 على الرابط:
http://doc.abhatoo.net.ma/IMG/doc/dro35.doc
41- يونس عرب، جرائم غسيل الأموال، منشور على موقع مندى كلية الحقوق، جامعة المنصورة، ت.د 2008/5/9، على الرابط:
http://www.f-law.net/law/showthread.php?t=8842
42- يونس عرب، ماهية ومخاطر غسيل الأموال، منشور على موقع حواس للمحاماة، وكذلك موقع مدونة مدينتي، ت.د 2/ 2008/5 على الرابطين:
http://hawassdroit.ibda3.org/montada-f17/topic-t420.htm
http://samirlawer.elaphblog.com/posts.aspx?U=995&A=6195

- مواقع تضمنت اتفاقيات وتقارير وقوانين وقضايا

1. تقرير وزارة الخارجية الأمريكية لعام 2007 حول الاتجار بالبشر منشور على موقع america.gov، ت.د 2008/1/20 على الرابط:
http://www.america.gov/st/washfile-arabic/2007/June/20070612124835ssissirdile0.5759546.html

2. تقرير لشركة مكافي المتخصصة في مجال الحماية الرقمية، التجسس على الإنترنت يتحول إلى حرب الكترونية، شبكة الإعلام العربية، ت.د 2008/6/10،على الرابط:

http://www.moheet.com/show_news.aspx?nid=61440&pg=10

3. تقرير دولي لشركة سيمنتيك لمكافحة الفيروسات، جريدة الشرق الأوسط الإلكترونية السعودية الصادرة يوم الخميس 30 ديسمبر 2004 على الرابط :

http://arabic.cnn.com/2006/scitech/4/26/emails.daily/index.html

4. الجريدة الرسمية الجزائرية، موقع الأمانة العامة للحكومة الجزائرية، ت.د2009/9/1 ،على الرابط :

http://www.joradp.dz/TRV/APenal.pdf

5. القانون الإماراتي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات منشور على موقع الشبكة العربية لمعلومات، ت.د 2006/12/2على لرابط:

http://www.openarab.net/laws/2006/laws8.shtml

6. نظام مكافحة الجرائم المعلوماتية السعودي منشور على موقع جريدة الوطن السعودية، ع 2674، الجمعة 16 محرم 1429 الموافق 25 يناير 2008،

http://www.alwatan.com.sa/news/newsdetail.asp?issueno=2674&id=39019&groupID=0

وموقع صحيفة سبرو الالكترونية على الرابط:

http://www.sabq.org/inf/news.php?action=show&id=4640

وموقع جوروسيديا موقع القانون المشارك، والموقع السوري للاستشارات والدراسات القانونية.

http://ar.jurispedia.org/index.php/%D9%86%D8%B8%D8%A7%D9%85_%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9_%D8%AC%D8%B1%D8%A7%D8%A6%D9%85_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9_(sa)

http://www.barasy.com/forum/showthread.php?t=1846

7. موقع متاح فيه قانون العقوبات القطري رقم (11)لسنة 2004، ت.د 2008/10/28 على الرابط :

http://62.215.234.226/MojPortalPublic/LawAsPDF.aspx?opt&country=3&LawID=2597

8. المرسوم السلطاني العماني، العماني رقم(72/ 2001) بشأن تعديل بعض أحكام قانون الجزاء العماني رقم (74/7)، منشور على موقع وزارة الشؤون القانونية العمانية، والرابط المتفرع عنه، ت.د 2009/11/4،على الرابطين:

http://www.mola.gov.om/legals.htm

http://www.mola.gov.om/legals/aljazaa_al3omani/amd3.pdf

9. التعاون في مجال مكافحة جرائم المعلوماتية بين الدول الأوربية، موقع قلم لذيذ lazeeez، شبكة الإنترنت، س .د 12، الأحد/2008/12/21على الرابط ص263

http://lazeeez.com/qalam/i-424-2342.html

10. قضية تحويل أموال إلكترونيا وبطرية غير مشروعة من بنوك في أمريكا إلى ماليزيا فاليمن صحيفة 26 سبتمبر، العدد 1103، وصحيفة الجمهورية، 14565، الاثنين 04 ديسمبر-كانون الأول 2006 على الرابطين:

http://www.26sep.net/newsweekarticle.php?lng=arabic&sid=7394

http://www.algomhoriah.net/newsweekarticle.php?sid=31021&page=1

11. قضية استدراج شخص من مدينة يمنية على أخرى عن طريق الإنترنت والقيام بقتلة، موقع المجلس اليمني، وموقع منتديات صوت القران، ت.د 27-12-2006، على الرابطين:

http://www.al-yemen.org/vb/archive/index.php/t-166743.html

/http://quran.maktoob.com/vb/quran9112

12. واقعة ضبط سيد يهات مخلة بالحياء، موقع صحيفة يمن نيوز على الرابط:

http://www.yemen-press.com/news572.html

13. قضية حيازة صور فتاة تحصل نتيجة اختراق بريدها الإلكتروني، ومن ثم القيام بتهديدها بنشر تلك الصور، صحيفة الوطن السعودية، الأحد 21-12-2008. ت.د على الرابط

http://www.almotamar.net/news/65627.htm.

14. طفل أردني يسطو إلكترونيا على عشرات البنوك والسحب من أرصدة عملاءها، موقع إنسان نت، ت.د 2008/8/6 على الرابط.

http://www.ensan.net/news/212/ARTICLE/3520/2008-04-18.html

15. عصابة دولية تخترق كمبيوترات من أنحاء العالم، موقع مجلة التقنية والاتصالات، 2009/11/14 على الرابط:

http://www.mnafe-it.com/index.php?id=155

16. اختراق موقع صحيفة الوطن السعودي، موقع مأرب برس، الأحد2009/11/8، على الرابط:

http://marebpress.net/news_details.php?sid=19910

17. موقع صحيفة العالم الرقمي ،الجزيرة ،ع 174، الأحد 12،رجب 1427 الموفق 8/6/ 2006، على الرابط:

http://www.al-jazirah.com/digimag/06082006/wr7.htm

18. قضية مشاهدة جريمة قتل عبر الانترنت جريدة الرياض الصادرة يوم الاثنين الموافق 12/ أكتوبر 2009، وموقع مدونات البوابة ت.د 2009/10/12على الرابط:

http://www.alriyadh.com/2009/10/12/article465633.html
http://blogs.albawaba.com/theoutsidersomali/67765/2009/10/12/189446-police-soccer-mom-video-chatting-when-shot

19.دور التعاون الدولي في اكتشاف وضبط عصابة مصرية أمريكية تقوم باختلاس الأموال وتحويلها عن طريق بطائق الائتمان، جريدة الحوادث المصرية، ت.د 2009/11/11 على الرابطين:

http://www.alarab.com.qa/admin/pdf/files/1556339366_Hawadeth1.pdf

20. واقعة اختراق صحيفة يمن نيوز والإجراءات التي تمت بشأنها، موقع الصحيفة، 09/12/12على الرابط:

/http://www.newsyemen.net
http://www.newsyemen.net/view_news.asp?sub_no=1_2009_12_05_40003

21. مقابلة أجرتها جريدة الشروق الجزائرية مع مسئولين في الدرك الوطني حول الإجرام المعلوماتي، وما زالت منشورة حتى 2009/9/10 على موقعها على الرابط:

http://www.echoroukonline.com/modules.php?name=News&file=article&sid=10731

- **مواقع باللغة الأجنبية:**

1. اتفاقية جنيف لعام 1937 المتعلقة بالمنع والقمع الدولي للإرهاب، منشورة على شبكة المعلومات الدولية، ت.ت2009/10/2، على الرابط:

https://www.unodc.org/tldb/pdf/Guide_Terr_Incorporation_Implementation_Ar.doc

2. موقع منشورة عليه الاتفاقية الدولية لمكافحة الأجرام المعلوماتي باللغة الفرنسية، تم التأكد من أنها لازالت منشورة في الموقع 2009/10/12 على الرابط:

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

3. موقع خاص ببعض القوانين الجنائية لعدد من الدول، يتفرع منه رابط خاص بقانون العقوبات الفرنسي

http://www.legislationline.org/upload/legislations/cd/1b/f05864013134135c992550ab7c98.htm.

4. رابط خاص بقانون الإجراءات الجزائية الفرنسي في موقع يتضمن عدد من القوانين العقابية والإجرائية الدولية ، ت.د 2009/4/20، على الرابط:

http://www.legislationline.org/documents/section/criminal-codes
legislationline.org/documents/section/criminel -codes

5. القانون الأمريكي لجرائم الحاسوب :
http://www.justice.gov/criminal/cybercrime/1030_new.html
6. دور التعاون الدولي في اكتشاف وضبط عصابة مصرية أمريكية تقوم باختلاس الأموال وتحويلها عن طريق بطائق الائتمان، موقع وزارة العدل الأمريكية، ت.د 2009/11/11 على الرابط:
http://www.justice.gov/criminal/cybercrime/cc.html#CC
7. قضية تبييض أموال باستخدام الوسائل الإلكترونية، من قبل مجموعة من مجرمي المعلوماتية بعد اختراق بطائق الائتمان لعدد من الشركات في الولايات المتحدة الأمريكية مشار إليها في موقع وزارة العدل الأمريكية، ت.د 2008/8/8 على الرابط:
http://www.usdoj.gov/criminal/cybercrime/index.html
8. Stéphanie Perrin, Cybercriminalité, article publié sur internet, date d'entrée 20/06/2009.
http://www.vecam.org/article657.html
9. Guy de Vel: Les défis de la cybercriminalité, étude réalisé à l'occasion de la conférence sur les défis de la cybercriminalité, organisée par le conseil de l'europe, Strasbourg, les 15-17 Septembre2007.
http://www.nouvellesmenaces.com/images/userFiles/Gendarmerie/File/Defis%20de%20la%20cybercriminalite%202004.pdf

الفـــــهـــــــــــرس

مفاتيح الكلمات

الكلمة	مفتاحها
قانون الجرائم والعقوبات اليمني	ق.ج. ع.ي
قانون العقوبات الجزائري	ق.ع.ج
عقوبات يمني	ع.ي
عقوبات جزائري	ع.ج
قانون العقوبات الفرنسي	ق.ع.ف
عقوبات فرنسي	ع.زف
قانون الإجراءات الجزائية اليمني	إ.ج.ي
إج راءات جزائية جزائري	إ.ج.ج
إجراءات جزائية فرنسي	إ.ج.ف
جزء	ج
طبعة أولى	ط1
دينار جزائري	د.ج
عدد	ع
تاريخ دخول الإنترنت أو إتاحة المعلومات	ت.د
رمز الدولار	$